Irēna Barkāne

Cilvēktiesību nozīme mākslīgā intelekta laikmetā

Privātums, datu aizsardzība un regulējums masveida novērošanas novēršanai

Cilvēktiesību nozīme mākslīgā intelekta laikmetā

Privātums, datu aizsardzība un regulējums masveida novērošanas novēršanai

Irēna Barkāne

Cilvēktiesību nozīme mākslīgā intelekta laikmetā

Privātums, datu aizsardzība un regulējums masveida novērošanas novēršanai

LU Akadēmiskais apgāds

UDK 34:004.8
Ba653

Irēna Barkāne. *Cilvēktiesību nozīme mākslīgā intelekta laikmetā. Privātums, datu aizsardzība un regulējums masveida novērošanas novēršanai.* Rīga: LU Akadēmiskais apgāds, 2023. 328 lpp.

Monogrāfija sagatavota un izdota ar Eiropas Reģionālā attīstības fonda darbības programmas "Izaugsme un nodarbinātība" specifiskā atbalsta mērķa 1.1.1.2. pasākuma "Pēcdoktorantūras pētniecības atbalsts" atbalstu projektā Nr. 1.1.1.2./VIAA1/1/16/196 "Taisnīgs līdzsvars starp privātumu un drošību kibertelpā: stingru datu aizsardzības standartu izveide Eiropā".

Monogrāfija atbalstīta izdošanai ar Latvijas Universitātes Humanitāro un sociālo zinātņu padomes 2021. gada 12. jūlija sēdes lēmumu (protokols Nr. 8).

LATVIJAS UNIVERSITĀTE

Recenzenti:

asociētais profesors *Dr*. Alesandro Mantelero (*Alessandro Mantelero*),
Turīnas Politehniskais institūts (*Polytechnic University of Turin*), Itālija;

asociētais profesors *Dr. iur*. Uldis Ķinis, Rīgas Stradiņa universitāte, Latvija

Latviešu valodas korektores Agita Kazakeviča un Ieva Zarāne

Angļu valodas korektori Andra Damberga,
Kristofers Godards (*Christopher Goddard*)

Maketu un vāka dizainu veidojusi Baiba Lazdiņa

ISBN 978-9934-36-097-8
ISBN 978-9934-36-098-5 (PDF)
https://doi.org/10.22364/cnmil.23

Monogrāfija veltīta mākslīgā intelekta tiesiskajiem un cilvēktiesību jautājumiem. Mākslīgais intelekts var sniegt ievērojamu labumu daudzās jomās, bet tas rada arī jaunus apdraudējumus. Viens no būtiskiem mākslīgā intelekta radītajiem izaicinājumiem ir mākslīgā intelekta novērošanas tehnoloģijas. Tās var aizskart cilvēka cieņu, tiesības uz privātumu un datu aizsardzību, diskriminācijas aizlieguma principu un pulcēšanās brīvību, kā arī apdraudēt tiesiskumu un demokrātiju. Gan Eiropā, gan visā pasaulē valstis, atsaucoties uz nacionālās drošības un sabiedrības drošības aizsardzības interesēm, strauji ievieš dažāda veida mākslīgā intelekta novērošanas tehnoloģijas. Sejas atpazīšanas tehnoloģijas, emociju uztveršanas tehnoloģijas, noziedzības prognozēšanas un automatizētu lēmumu pieņemšanas sistēmas ir radījušas plašas diskusijas par to ētisko, tiesisko un sociālo ietekmi un nepieciešamību ierobežot un aizliegt to izmantošanu. Esošais tiesiskais regulējums, īpaši cilvēktiesības un datu aizsardzības tiesības, jau šobrīd regulē mākslīgā intelekta tehnoloģijas, kā arī tiek izstrādāts jauns mākslīgā intelekta regulējums, ko ir nepieciešams izvērtēt.

Grāmatā vispirms ir apskatīta mākslīgā intelekta novērošanas tehnoloģiju izmantošana tiesībaizsardzības jomā Eiropā un pasaulē un izvērtēta to ietekme uz cilvēktiesībām. Pēc tam tajā ir aplūkotas tiesības uz privātumu, datu aizsardzības tiesības, kā arī mākslīgā intelekta regulējuma attīstība starptautiskā un Eiropas līmenī. Grāmatas turpinājumā ir analizēti Eiropas Cilvēktiesību tiesas un Eiropas Savienības Tiesas praksē izstrādātie nosacījumi tiesību uz privātumu un datu aizsardzību ierobežošanai un Eiropas datu aizsardzības prasības, kas piemērojamas mākslīgā intelekta novērošanas pasākumiem. Nobeigumā ir sniegtas rekomendācijas mākslīgā intelekta tiesiskā regulējuma un politikas tālākai attīstībai, kas būtu balstīta cilvēktiesībās un noteiktu efektīvas aizsardzības garantijas un mehānismus, kā arī ierobežojumus un aizliegumus, lai nodrošinātu mākslīgā intelekta tehnoloģiju atbildīgu un uzticamu izmantošanu un novērstu to radīto apdraudējumu un masveida novērošanu.

Grāmata būs noderīga mācībspēkiem un zinātniekiem, studentiem, tiesību piemērotājiem un digitālās politikas veidotājiem, iestādēm un uzņēmumiem, kas izstrādā, ievieš un izmanto mākslīgā intelekta tehnoloģijas, kā arī ikvienam lasītājam, kuram ir interese par cilvēktiesībām, datu aizsardzības tiesībām, Eiropas Savienības tiesībām, mākslīgā intelekta un jauno tehnoloģiju regulējuma attīstību.

Saturs

6. DAĻA

7. DAĻA

SUMMARY

IZMANTOTIE SAĪSINĀJUMI

AHEG	*UNESCO Ad Hoc Expert Group (AHEG) for the preparation of a draft text of a Recommendation on the Ethics of Artificial Intelligence* – angļu val.; UNESCO Starptautiskā *ad hoc* ekspertu grupa Rekomendācijas par mākslīgā intelekta ētiku izstrādei
AI HLEG	*High-Level Expert Group on Artificial Intelligence set up by the European Commission* – angļu val.; Eiropas Komisijas izveidota augsta līmeņa ekspertu grupa mākslīgā intelekta jautājumu risināšanai
ANO	Apvienoto Nāciju Organizācija
CAHAI	*Ad hoc Committee on Artificial Intelligence of the Council of Europe* – angļu val.; Eiropas Padomes Mākslīgā intelekta *ad hoc* komiteja
CCTV	*Closed-circuit television* – angļu val.; videonovērošanas kameras/ sistēma
CNIL	*Commission Nationale de l'Informatique et des Libertés* – franču val.; Francijas datu aizsardzības iestāde
Direktīva 95/46/EK	Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti
ECT	Eiropas Cilvēktiesību tiesa
ECTK	Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija
EDRi	*European Digital Rights* – angļu val.; Eiropas Digitālo tiesību asociācija
Eiropols	Eiropas Savienības Aģentūra tiesībaizsardzības sadarbībai
ENISA	Eiropas Savienības Kiberdrošības aģentūra
E-privātuma direktīva	Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju)
E-privātuma regulas priekšlikums	Eiropas Komisijas priekšlikums Eiropas Parlamenta un Padomes regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula)
EST	Eiropas Savienības Tiesa
FPDAL	Fizisko personu datu apstrādes likums
FRA	*European Union Agency for Fundamental Rights* – angļu val.; Eiropas Savienības Pamattiesību aģentūra
Harta	Eiropas Savienības Pamattiesību harta

ICO	*The Information Commissioner's Office* – angļu val.; Apvienotās Karalistes Informācijas komisāra birojs
Konvencija 108	Eiropas Padomes Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi
Konvencija 108+	Eiropas Padomes modernizētā Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi
LES	Līgums par Eiropas Savienību
LESD	Līgums par Eiropas Savienības darbību
MI akta priekšlikums	Eiropas Komisijas priekšlikums Eiropas Parlamenta un Padomes regulai, kas nosaka saskaņotas normas mākslīgā intelekta jomā (Mākslīgā intelekta akts) un groza dažus Savienības leģislatīvos aktus
MI ētikas vadlīnijas	AI HLEG Ētikas vadlīnijas uzticamam mākslīgajam intelektam
NIS direktīva	Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā
NSA	*National Security Agency* – angļu val.; ASV Nacionālās drošības aģentūra
OECD	*Organisation for Economic Co-operation and Development* – angļu val.; Ekonomiskās sadarbības un attīstības organizācija
OHCHR	*The Office of the United Nations High Commissioner for Human Rights* – angļu val.; Apvienoto Nāciju Organizācijas Augstā cilvēktiesību komisāra birojs
Policijas direktīva	Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI
Satversme	Latvijas Republikas Satversme
SPPPT	Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām
UNESCO	*United Nations Educational, Scientific and Cultural Organisation* – angļu val.; Apvienoto Nāciju Izglītības, zinātnes un kultūras organizācija
UNICEF	*The United Nations International Children's Emergency Fund* – angļu. val.; ANO Bērnu fonds
UNICRI	*United Nations Interregional Crime and Justice Research Institute* – angļu val.; ANO Starpreģionālās noziedzības un tieslietu pētniecības institūts
VDAR	Vispārīgā datu aizsardzības regula

IEVADS

Mākslīgā intelekta attīstība notiek ļoti strauji. Tas lielā mērā pārveido sabiedrību un var sniegt nozīmīgus ieguvumus daudzās jomās, to skaitā zinātnes, izglītības, transporta, nodarbinātības, kultūras, veselības, tiesībaizsardzības un drošības jomā, bet vienlaikus tas rada arī daudz jaunu izaicinājumu. Viens no lielākajiem izaicinājumiem ir mākslīgā intelekta novērošanas tehnoloģijas, kas rada būtisku apdraudējumu cilvēktiesībām, tiesiskumam un demokrātijai.

Arvien vairāk valstu visā pasaulē izmanto mākslīgā intelekta novērošanas tehnoloģijas – sejas atpazīšanas sistēmas, automatizētu lēmumu pieņemšanas un prognozēšanas sistēmas, automatizētas robežkontroles sistēmas utt.[1] Visplašākās diskusijas, kā arī kritiku ir radījušas sejas atpazīšanas tehnoloģijas, to izmantošana strauji pieaug gan valsts, gan privātā sektorā. Daudzās Eiropas valstīs, piemēram, Lielbritānijā, Francijā, Vācijā, Spānijā, Nīderlandē, tās arvien vairāk izmanto policija un citas tiesībaizsardzības iestādes, bieži vien slepenā un nekontrolētā veidā. Tās ievieš arī citas publiskas iestādes un privātie uzņēmumi, lai veiktu novērošanu, piemēram, darbā, skolās, lielveikalos, lidostās, sporta pasākumos utt.

Starptautiskās organizācijas, valstu likumdevēji, uzraudzības iestādes, nevalstiskās organizācijas, cilvēktiesību aizstāvji un zinātnieki arvien vairāk uzsver nepieciešamību regulēt vai pat aizliegt šo tehnoloģiju izmantošanu. 2019. gadā Sanfrancisko bija pirmā Amerikas Savienoto Valstu pilsēta, kas aizliedza šīs tehnoloģijas izmantot policijas un valsts iestādēm. Drīz arī citas ASV pilsētas, to skaitā Oklenda, Bostona, Mineapolisa, pieņēma līdzīgus noteikumus, ņemot vērā, ka daudzos gadījumus šīs tehnoloģijas atspoguļo aizspriedumus, piemēram, pēc rases, vecuma un etniskās piederības, un ir diskriminējošas.[2]

Arī Eiropā tiek plaši diskutēts, kā regulēt un ierobežot sejas atpazīšanas tehnoloģiju izmantošanu. Eiropas Padome ir mudinājusi izstrādāt un pieņemt speciālu regulējumu attiecībā uz sejas atpazīšanas tehnoloģiju biometrisko apstrādi, ko veic

1 Feldstein, S. (2019). The Global Expansion of AI surveillance. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

2 Ravani, S. (17 July, 2019). Oakland bans use of facial recognition technology, citing bias concerns. *San Francisco Chronicle.* https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php; Lyons, K. (13 February, 2021). Minneapolis prohibits use of facial recognition software by its police department. *The Verge.* https://www.theverge.com/2021/2/13/22281523/minneapolis-prohibits-facial-recognition-software-police-privacy

valsts iestādes tiesībaizsardzības nolūkos, kā arī aizliegt konkrētus to izmantošanas veidus.[3] Eiropas Savienība izstrādā mākslīgā intelekta regulējumu, kurā īpaša uzmanība ir pievērsta biometrisko datu izmantošanai attālinātai identifikācijai tiesībaizsardzības nolūkos. Eiropas Komisijas 2020. gadā publicētajā Baltajā grāmatā par mākslīgo intelektu ir uzsvērts, ka biometrisko datu izmantošana un vākšana attālinātās identifikācijas nolūkos rada specifiskus riskus cilvēka cieņai, tiesībām uz privāto dzīvi un personas datu aizsardzību, kā arī citām pamattiesībām.[4]

2021. gada 21. aprīlī Eiropas Komisija nāca klajā ar jaunu Mākslīgā intelekta regulas priekšlikumu (MI akta priekšlikums).[5] Tas ir pasaulē pirmais priekšlikums, kas paredz mākslīgā intelekta jomas tiesisko regulējumu. MI akta priekšlikums nosaka konkrētu mākslīgā intelektā balstītas prakses veidu aizliegumu. Līdzās citiem aizliegumiem, piemēram, sociālajai novērtēšanai, kaitīgai manipulēšanai un personas uzvedības ietekmēšanai, ir paredzēts aizliegt arī reāllaika biometrisko attālinātās identifikācijas sistēmu izmantošanu sabiedriskās vietās tiesībaizsardzības nolūkos. Tomēr šo aizliegumu piemērošana ir ierobežota, kā arī ir paredzēti daudzi izņēmumi. MI akta priekšlikumā ietvertos noteikumus ir kritizējuši Eiropas Datu aizsardzības uzraudzītājs un Eiropas Datu aizsardzības kolēģija, aicinot aizliegt mākslīgā intelekta izmantošanu, lai automātiski atpazītu cilvēka pazīmes sabiedriskās vietās.[6]

Sejas atpazīšanas tehnoloģijas ir nonākušas arī Eiropas datu aizsardzības iestāžu redzeslokā. Francijas un Zviedrijas datu aizsardzības iestādes ir atzinušas, ka to izmantošana skolās pārkāpj Eiropas datu aizsardzības regulējumu.[7]

3 Council of Europe. (2021). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). Guidelines on Facial Recognition. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

4 Eiropas Komisija. (2020). Baltā grāmata par mākslīgo intelektu. Eiropiska pieeja – izcilība un uzticēšanās. https://op.europa.eu/lv/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

5 Eiropas Komisija. (2021). Priekšlikums. Eiropas Parlamenta un Padomes Regula, kas nosaka saskaņotas normas mākslīgā intelekta jomā (Mākslīgā intelekta akts) un groza dažus Savienības leģislatīvos aktus. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

6 EDPB, EDPS. (2021). EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https:// https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en

7 EDPB. (22 August, 2019). Facial recognition in school renders Sweden's first GDPR fine. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-zfirst-gdpr-fine_en; CNIL. (29 Octobre, 2019). Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.

Zviedrijas datu aizsardzības iestāde arī ir konstatējusi, ka Zviedrijas policija, izmantodama "Clearview AI" personu identificēšanai, ir pārkāpusi datu aizsardzības noteikumus.[8]

Pret sejas atpazīšanas tehnoloģiju izmantošanu sabiedriskās vietās arvien skaļāk iebilst nevalstiskās organizācijas. 2020. gada novembrī Eiropas Digitālo tiesību asociācija (EDRi) – Eiropas nevalstisko organizāciju tīkls, kas aizstāv pamattiesības digitālajā vidē, – uzsāka kampaņu "Atgūsti savu seju" (*Reclaim Your face* – angļu val.). 2021. gada februārī asociācija ierosināja Eiropas Pilsoņu iniciatīvu, aicinot Eiropas Komisiju stingri reglamentēt biometrisko tehnoloģiju izmantošanu un aizliegt šo tehnoloģiju, it īpaši sejas atpazīšanas tehnoloģiju, izmantošanu sabiedriskās vietās, jo tās var izraisīt nelikumīgu masveida novērošanu un ir pretrunā cilvēktiesībām.[9]

Ne tikai sejas atpazīšanas tehnoloģijas ir raisījušas lielas bažas par to ietekmi uz cilvēktiesībām un tiesiskumu. Satraukumu ir radījušas arī citas mākslīgā intelekta novērošanas tehnoloģijas, kas tiek izmantotas, ne tikai lai atpazītu sejas, bet arī lai novērotu emocijas un uzvedību, un to izmantošana profilēšanai un prognozēšanai.[10] Pēdējos gados visā pasaulē strauji pieaug tendence izmantot biometriskās tehnoloģijas. Biometriskās un emocionālās atpazīšanas tehnoloģijas arvien vairāk izmanto tiesībaizsardzības iestādes Eiropas valstīs, turklāt nenodrošinot pārredzamību, uzraudzību un sabiedrības līdzdalību. Biometriskās novērošanas tehnoloģijas, piemēram, sejas atpazīšana un algoritmiskās profilēšanas un prognozēšanas rīki, tiek testēti uz Eiropas robežām. Plašu kritiku izraisīja ES finansētais projekts "iBorderCtrl", kurā tika plānots testēt melu noteikšanas sistēmu imigrācijas kontrolei.[11] Sejas atpazīšanas tehnoloģijas tiesībaizsardzības iestādes un policija izmanto arī prognozēšanai, kas var balstīties uz iedzīvotāju uzvedības analīzi un vērtēšanu, lai apkarotu noziedzību. ES Mākslīgā intelekta augsta līmeņa ekspertu grupa (AI HLEG) ir uzsvērusi, ka

8 EDPB. (21 February, 2021). Swedish DPA: Police unlawfully used facial recognition app. https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_lv

9 EDRi. (17 February, 2021). New ECI calls Europeans to stand together for a future free from harmful biometric mass surveillance. https://edri.org/our-work/new-eci-ban-biometric-mass-surveillance/

10 Sk., piemēram, Mcstay, A. (2020). Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy, *Big Data & Society*, 7(1). https://doi.org/10.1177/2053951720904386

11 Stolton, S. (8 February, 2021). Commission under pressure in EU court over 'lie detector tech'. *EURACTIV* https://www.euractiv.com/section/digital/news/aommission-under-pressure-over-lie-detector-tech-in-eu-courts/. Sk. arī Gallagher, R., Jona, L. (26 July, 2019). We tested Europe's new lie detector for travelers – and immediately triggered a false positive. *The Intercept*. https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/

fizisku personu identificēšana, izmantojot biometriskos datus, piemēram, melu atpazīšana un personības vērtēšana, izmantojot mikroizteiksmes, un automātiskā balss atpazīšana, rada būtiskus tiesiskus un ētiskus izaicinājumus.[12] Lielu satraukumu ir radījusi arī policijas un tiesībaizsardzības iestāžu prakse arvien vairāk paļauties uz mākslīgā intelekta datu analīzes un prognozēšanas rīkiem, lai novērstu un kontrolētu noziedzību.[13]

Jau ilgstoši pastāv plašas diskusijas par robežām, cik tālu valsts var izmantot datu vākšanas un analīzes metodes un tehnoloģijas, lai veiktu novērošanu, lai aizsargātu tādas sabiedrības intereses kā valsts un sabiedrības drošība. Arvien pieaugošie drošības draudi ir veicinājuši masveida novērošanas praksi visā pasaulē. Edvarda Snoudena (*Edward Snowden*) atklājumi par ASV īstenoto slepeno masveida novērošanas programmu, kas tika ieviesta pēc 11. septembra teroraktiem un paredzēja plašu gan ASV pilsoņu, gan citu valstu, to skaitā Eiropas, iedzīvotāju telekomunikācijas un datu plūsmas novērošanu un pārtveršanu iepriekš neiedomājamos apmēros, aizsāka plašu globālu diskusiju par izlūkdienestu un tiesībaizsardzības iestāžu masveida novērošanas praksi, tās radīto būtisko aizskārumu cilvēktiesībām, īpaši tiesībām uz privātumu un datu aizsardzību, atbilstoša regulējuma trūkumu, kā arī efektīvu aizsardzības garantiju neesamību.[14]

Ne tikai ASV, bet arī Eiropā ir ieviesta plaša masveida novērošanas prakse, piemērojot dažāda veida pasākumus drošības nolūkos. Eiropas Savienības Tiesai (EST) un Eiropas Cilvēktiesību tiesai (ECT) līdz šim ir bijusi izšķiroša nozīme masveida novērošanas ierobežošanā un uzraudzībā, veicinot tiesību uz privātumu, datu aizsardzību un citu cilvēktiesību ievērošanu un aizsardzību.[15]

ES līmenī arī ir ieviesti daudzi masveida novērošanas pasākumi drošības interešu vārdā. Kā steidzams pretterorisma pasākums, reaģējot uz teroristu uzbrukumiem 2004. gadā Madridē un 2005. gadā Londonā, 2006. gadā ātri tika pieņemta

12 AI HLEG. (2019). Ethics Guidelines for Trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

13 Sk. McDaniel, J. L. M., Pease, K. G. (2021). Introduction. In: McDaniel, J. L. M., Pease, K. G. (eds.), *Predictive Policing and Artificial Intelligence*. Routledge, pp. 1–38; van Brakel, R. E. (2021). Rethinking predictive policing: Towards a holistic framework of democratic algorithmic surveillance. In: Schuilenburg, M., Peeters, R. (eds.), *Algorithmic Societies: Power, Knowledge and Technology in the Age of Algorithms*. Routledge, pp. 104–118.

14 Sk., piemēram, OHCHR. (2014). The right to privacy in the digital age. https://digitallibrary.un.org/record/777869

15 Sk. Nesterova, I. (2019). Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards. In: Ulrich, G., Ziemele, I. (eds.), *How International Law Works in Times of Crisis*. Oxford University Press, pp. 109–125.

ES Datu saglabāšanas direktīva[16], neņemot vērā iebildumus par tās neatbilstību pamattiesībām. 2014. gadā EST pieņēma spriedumu apvienotajās lietās "Digital Rights Ireland" un "Seitlinger u. c.", ar kuru pasludināja minēto direktīvu par spēkā neesošu, atzīstot, ka ar to uzliktais pienākums valstīm paredzēt, ka elektronisko pakalpojumu sniedzējiem ir jāsaglabā noteiktu kategoriju dati, rada nepamatotu iejaukšanos pamattiesībās.[17]

EST ir pieņēmusi vairākus spriedumus, kuriem par pamatu ir ASV masveida novērošanas prakse. Tā 2015. gadā pieņēma spriedumu "Schrems I" lietā[18] un 2020. gadā – "Schrems II" lietā[19], ar kuriem divas reizes atzina par spēkā neesošiem Eiropas Komisijas lēmumus par aizsardzības līmeņa pietiekamību datu nodošanai no ES uz ASV. Arī ECT ilgstoši turpina izskatīt daudzas lietas par valstu masveida novērošanas pasākumu atbilstību cilvēktiesībām, mēģinot noteikt robežas, cik tālu ir ierobežojamas personas tiesības uz privātumu, atsaucoties uz valsts un nacionālās drošības interesēm.[20] Plašā tiesu prakse apliecina, ka atcelt masveida novērošanas pasākumus, kas drošības nolūkos tiek ieviesti gan ES, gan nacionālā līmenī, ir ļoti grūti, un bieži vien tas ir iespējams tikai pēc ilgstošiem tiesvedības procesiem.

Līdzīgi kā terorisma un drošības draudi vēl lielākus jaunu novērošanas tehnoloģiju "plūdus" izraisīja Covid-19 krīze. Lai cīnītos ar pandēmijas izplatību, valstis visā pasaulē strauji ieviesa digitālās novērošanas tehnoloģijas, sākot no veselības lietotnēm, valkājamām aprocēm, kontaktu izsekošanas un citām mobilām lietotnēm un beidzot ar droniem un sejas atpazīšanas tehnoloģijām.[21] Šie eksperimenti ir būtiski satricinājuši cilvēktiesības, radot jaunus jautājumus, cik tālu var ierobežot privātumu, datu aizsardzību un citas cilvēktiesības, lai garantētu sabiedrības veselību un drošību, un kā līdzsvarot indivīda un sabiedrības intereses. Ārkārtas apstākļi neatceļ cilvēktiesību ievērošanas prasību.

16 Eiropas Parlamenta un Padomes Direktīva 2006/24/EK (2006. gada 15. marts) par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK. *OV L* 105, 13.04.2006. (spēkā līdz 03.05.2006.).

17 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C293/12 *Digital Rights Ireland* un C594/12 *Seitlinger* u. c., ECLI:EU:C:2014:238.

18 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems* pret *Data Protection Commissioner,* ECLI:EU:C:2015:650.

19 EST 2020. gada 16. jūlija spriedums lietā C-311/18 *Data Protection Commissioner pret Facebook Ireland Limited* un *Maximillian Schrems,* ECLI:EU:C:2020:559.

20 Sk. European Court of Human Rights. (2020). Guide on Article 8 of the Convention – Right to respect for private and family life https://www.echr.coe.int/documents/guide_art_8_eng.pdf

21 Couch, D. L., Robinson, P., and Komesaroff, P. A. (2020). COVID-19 – Extending Surveillance and the Panopticon. *Journal of Bioethical Inquiry*, 17, pp. 809–814. https://doi.org/10.1007/s11673-020-10036-5

Ir ārkārtīgi svarīgi steidzami risināt tiesiskos, ētiskos un sociālos jautājumus, kas saistīti ar mākslīgā intelekta un citu novērošanas tehnoloģiju izmantošanu. Tās var radīt jauna veida apdraudējumu cilvēktiesībām, ievērojami veicināt sabiedrības kontroli, balstoties uz tādiem mērķiem un vērtībām, kas var būt pretrunā ar demokrātiskas sabiedrības vērtībām. Ķīnas sociālā vērtēšanas un tā saucamā "sociālā kredīta" sistēma ir šīs tendences spilgtākais piemērs.[22]

Mākslīgā intelekta novērošanas tehnoloģijas atšķiras no iepriekšējām digitālās novērošanas formām. Mākslīgais intelekts piedāvā jaunas iespējas datu vākšanai, apstrādei un analīzei, ļauj veikt novērošanu daudz plašāk, detalizētāk un precīzāk, tādējādi ievērojami veicinot novērošanas pasākumu izmantošanu. Šīs tehnoloģijas rada jauna veida specifiskus apdraudējumus. Tās būtiski apdraud tiesības uz privātumu un datu aizsardzību, cilvēka cieņu un diskriminācijas aizlieguma principu, vārda un pulcēšanās brīvību un citas cilvēktiesības un brīvības, kā arī rada plašāku ietekmi uz sabiedrību, tiesiskumu un demokrātiju kopumā.[23] Mākslīgais intelekts ievērojami palielina gan valsts, gan lielo tehnoloģiju uzņēmumu masveida novērošanas apmērus un saasina varas nevienlīdzību. Grāmatas "Uzraudzības kapitālisma laikmets. Cīņa par cilvēka nākotni jaunajās varas robežās" autore Šošana Zubofa (*Shoshana Zuboff*) vērš uzmanību, ka novērošanas kapitālisms izraisa katastrofālas sekas demokrātijai un brīvībai, jo rada vēl nebijušu zināšanu un varas koncentrāciju, ko neregulē likumi un noteikumi. Šī zināšanu un varas asimetrija izraisa jaunas sociālās nevienlīdzības formas, ļauj ietekmēt indivīdu un iedzīvotāju uzvedību, kas ir antidemokrātiski.[24] Lai gan šī grāmata pamatā ir veltīta valsts masveida novērošanai un komerciālā novērošana ir ārpus tās pētāmo jautājumu loka, tajā pašā laikā izaicinājumi, ko rada komerciālā novērošana, it īpaši sociālo mediju platformu algoritmi, kas ietekmē un manipulē ar lietotāju viedokli un sociālo un politisko uzvedību, ir ne mazāk būtiski, un tiem būtu veltāms atsevišķs pētījums.

Lai nodrošinātu, ka mākslīgā intelekta novērošanas tehnoloģiju izmantošana atbilst cilvēktiesībām un tās neapdraud, ir ļoti svarīgi steidzami izvērtēt esošo

22 Kobie, N. (7 June, 2019). The Complicated truth about China's social credit system. *WIRED.* https://www.wired.co.uk/article/china-social-credit-system-explained

23 Sk. Council of Europe, CAHAI Secretariat. (2020). Towards regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law. https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a

24 Sk. Zuboff, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the new Frontier of Power.* Profile Books, pp. 512–519. Sk. arī Naughton, J. (20 January, 2019). 'The goal is to automate us': welcome to the age of surveillance capitalism. *The Guardian.* https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

regulējumu, kā arī izstrādāt jaunu regulējumu, kas noteiktu skaidras robežas, kādos gadījumos mākslīgā intelekta tehnoloģijas var izmantot un kādos nevar, un kas paredzētu efektīvas aizsardzības garantijas un uzraudzības mehānismus. Steidzami ir jānosaka ierobežojumi mākslīgā intelekta novērošanas pasākumiem, lai garantētu līdzsvaru starp valsts un sabiedrības drošību, no vienas puses, un nepieciešamību aizsargāt cilvēktiesības un demokrātiju, no otras puses. Regulējums ir būtisks instruments, lai nodrošinātu atbildīgu un uz cilvēkiem vērstu mākslīgā intelekta izmantošanu un novērstu tā radīto apdraudējumu.

Pēdējo gadu laikā starptautiskās organizācijas, it īpaši Eiropas Padome[25], Apvienoto Nāciju Izglītības, zinātnes un kultūras organizācija (UNESCO)[26], Ekonomiskās sadarbības un attīstības organizācija (OECD)[27], ES[28], daudzas profesionālās organizācijas[29], nevalstiskās un citas organizācijas, kā arī tehnoloģiju uzņēmumi[30] strauji izstrādājuši un turpina izstrādāt mākslīgā intelekta ētikas vadlīnijas, lai definētu vērtības, principus un ietvaru ētiskai mākslīgā intelekta attīstībai. Tomēr arvien skaidrāk tiek uzsvērts, ka regulējumam ir jāiet tālāk par ētikas normām un gan starptautiskā, gan nacionālā līmenī ir jānosaka tiesiski saistošas prasības un jāievieš efektīvi praktiski mehānismi, kas nodrošinātu šo ētikas principu ieviešanu praksē. Gan starptautiskās organizācijas, gan valstis visā pasaulē šobrīd aktīvi meklē labāko veidu, kā tiesiski regulēt mākslīgo intelektu.

Tajā pašā laikā spēkā esošais tiesiskais regulējums, it sevišķi cilvēktiesību un datu aizsardzības regulējums, jau šobrīd ir piemērojams attiecībā uz mākslīgo intelektu. Cilvēka cieņa, tiesības uz privātumu un datu aizsardzību, diskriminācijas aizlieguma princips, vārda un pulcēšanās brīvība, kā arī citas cilvēka tiesības un brīvības ir īpaši nozīmīgas un piemērojamas attiecībā uz mākslīgā intelekta

25 Council of Europe. (2020). Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

26 UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137

27 OECD. (2019). Recommendation of the Council on Artificial Intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

28 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

29 Sk., piemēram, IEEE. (2019). Ethically Aligned Design. First Edition: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf?utm_medium=undefined&utm_source=undefined&utm_campaign=undefined&utm_content=undefined&utm_term=undefined

30 Sk. Fjeld, J., Achten, N., Hilligoss, H., et al. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Berkman Klein Center Research Publication No. 2020-1. https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y

novērošanas tehnoloģijām un var palīdzēt noteikt to izmantošanas tā sauktās sarkanās līnijas. Būtiskas prasības mākslīgā intelekta sistēmu izstrādei, ieviešanai un izmantošanai nosaka arī datu aizsardzības regulējums, it īpaši Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)[31] un Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīva (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu kriminālsodus, un par šādu datu brīvu apriti[32] (Policijas direktīva; *Law Enforcement Directive* – angļu val.), kura paredz datu vākšanas un izmantošanas noteikumus un stingras atbildības prasības.

Grāmatā tiek izvirzīta tēze, ka cilvēktiesību un datu aizsardzības standarti ir visdrošākais pamats mākslīgā intelekta regulējuma turpmākai attīstībai un ir nepieciešams izstrādāt skaidru tiesisko regulējumu, kas tālāk attīstītu starptautiskās cilvēktiesību normas un Eiropas datu aizsardzības regulējumu un noteiktu skaidrus mākslīgā intelekta novērošanas tehnoloģiju izmantošanas ierobežojumus. Tāpēc ir jāizvērtē esošā tiesiskā regulējuma atbilstība, efektivitāte un trūkumi un pēc tam jāapsver jauna regulējuma nepieciešamība. Jauns tiesiskais regulējums būtu jāpieņem tikai tad, kad jautājums ir pienācīgi izprasts, ir notikušas sabiedriskās diskusijas un ir konstatēts, ka spēkā esošie likumi nav pietiekami, lai risinātu noteiktus jautājumus.

Grāmatas mērķis ir izpētīt mākslīgā intelekta novērošanas tehnoloģiju ietekmi uz cilvēktiesībām, tām piemērojamo spēkā esošo regulējumu un tā turpmāko attīstību nākotnē, lai novērstu šo tehnoloģiju radītos riskus un apdraudējumu.

Monogrāfija ir pirmais zinātniskais pētījums Latvijas tiesību zinātnē, kurā analizēta un pētīta mākslīgā intelekta ietekme uz cilvēktiesībām un tiesiskais regulējums, kā arī novērošanas tehnoloģiju radītie riski un apdraudējums. Tā sniedz ieteikumus turpmākai regulējuma un politikas attīstībai starptautiskā un nacionālā līmenī.

31 Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (Dokuments attiecas uz EEZ). *OV L* 119, 04.05.2016.

32 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu kriminālsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI. *OV L* 119, 04.05.2016.

Grāmatā ir aplūkota mākslīgā intelekta novērošanas tehnoloģiju izmantošana tiesībaizsardzības jomā un to attīstības tendences gan Eiropā, gan citviet pasaulē un izvērtēts šo tehnoloģiju radītais apdraudējums cilvēktiesībām, kā arī ietekme uz sabiedrību un demokrātiju kopumā. Autore apskata, kā attīstās mākslīgā intelekta regulējums, lai ierobežotu novērošanas tehnoloģiju radītos riskus, un kā esošais cilvēktiesību un datu aizsardzības regulējums jau šobrīd regulē šīs tehnoloģijas. Tajā ir analizēts, kā tiesības uz privātumu un datu aizsardzību un to ierobežošanas nosacījumi, kas attīstīti ECT un EST praksē, ir piemērojami attiecībā uz mākslīgā intelekta novērošanas pasākumiem. Grāmata sniedz rekomendācijas, kā attīstīt mākslīgā intelekta novērošanas tehnoloģiju tiesisko regulējumu un kādas aizsardzības garantijas un mehānismi jāievieš praksē, lai nodrošinātu atbildīgu un uz cilvēku vērstu šo tehnoloģiju izmantošanu un novērstu to radīto apdraudējumu.

Grāmatā ir plaši analizēti Latvijas, starptautiskie un ārvalstu tiesību akti, instrumenti, politikas dokumenti un tiesu prakse, kā arī citi prakses materiāli. Būtiska nozīme monogrāfijā ir cilvēktiesību, datu aizsardzības, kā arī mākslīgā intelekta jomā tādu pieņemto tiesību aktu, vadlīniju un cita veida dokumentu analīzei, ko ir pieņēmušas vai šobrīd izstrādā ES, Eiropas Padome, ANO, UNESCO un OECD. Darbā ir izmantoti Eiropas valsts iestāžu, datu aizsardzības iestāžu un citu valsts institūciju, nevalstisko organizāciju izstrādātie dokumenti (piemēram, EDRi[33]), pētniecības institūtu (piemēram, Berkmana Kleina centra[34], *AI Now* institūta[35], Alana Tjūringa institūta[36]), Eiropas Savienības Pamattiesību aģentūras (FRA)[37] pētījumi. Tāpat darbā ir izmantoti dokumenti, ko izstrādājušas starptautiskās mākslīgā intelekta ekspertu grupas: Eiropas Padomes Mākslīgā intelekta *ad hoc* komiteja (CAHAI)[38], ES AI HLEG[39] un UNESCO Starptautiskā *ad hoc* ekspertu

33 EDRi. (12 January, 2021). Re: Open letter: Civil society call for the introduction of red lines in the upcoming European Commission proposal on Artificial Intelligence. https://edri.org/wp-content/uploads/2021/01/EDRi-open-letter-AI-red-lines.pdf

34 Fjeld, et al. (2020), Principled Artificial Intelligence.

35 Crawford, K., Roel, D., Theodora, D., et al. (2019). AI Now 2019 Report. New York, AI Now Institute. https://ainowinstitute.org/publication/ai-now-2019-report-2

36 Leslie D. (2020). Understanding bias in facial recognition technologies: an explainer. The Alan Turing Institute. https://doi.org/10.5281/zenodo.4050457

37 FRA. (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement. https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

38 Council of Europe, CAHAI. (2020). Feasibility Study. https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

39 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

grupa Rekomendācijas par mākslīgā intelekta ētiku izstrādei (AHEG)[40]. Grāmatā ir arī plaši analizēta un salīdzināta ECT un EST judikatūra. Lai gan galvenokārt ir analizēti mākslīgā intelekta tiesiskie aspekti, darbā plaši izmantota starpdisciplinārā pieeja. Lai izprastu mākslīgā intelekta novērošanas sistēmas un atklātu ne tikai to tiesisko, bet arī sociālo un ētisko ietekmi, kā arī ietekmi uz sabiedrību un demokrātiju, līdzās pētījumiem tiesību zinātnē ir izmantots plašs klāsts pētījumu (grāmatu, zinātnisko rakstu, ziņojumu un citu dokumentu) socioloģijā, ētikā, filozofijā, politikā, tehnoloģijā un citās jomās.

Grāmatas mērķauditorija ir plaša. Tā būs noderīgs materiāls tiesību zinātņu un citu sociālo un humanitāro zinātņu, kā arī tehnoloģiju, dabaszinātņu un medicīnas zinātņu pētniekiem un akadēmiskajiem mācībspēkiem, kā arī studentiem. Pētījuma rezultāti un politikas ieteikumi būs vērtīgs informācijas avots likumdevējam, kā arī tiesām un citām valsts, tiesībaizsardzības un uzraudzības institūcijām, lai izstrādātu regulējumu un politiku, ieviestu uzraudzības pasākumus un atbildības mehānismus uzticamam mākslīgajam intelektam un veicinātu tiesisku, ētisku, atbildīgu un uz cilvēku vērstu mākslīgā intelekta attīstību. Pētījums var būt noderīgs iestādēm un uzņēmumiem, kas izstrādā, ievieš un izmanto mākslīgā intelekta un citas jaunās tehnoloģijas, un nevalstiskajām organizācijām, lai veicinātu sabiedrības iesaisti un informētu par mākslīgā intelekta un citu jauno tehnoloģiju ietekmi uz cilvēktiesībām, to radītajiem riskiem un apdraudējumu. Visbeidzot, grāmata ir paredzēta ikvienam lasītājam, kurš vēlas uzzināt vairāk par mākslīgā intelekta regulējuma attīstību, tā ietekmi uz cilvēktiesībām un datu aizsardzības tiesībām.

Temats tiek apskatīts septiņās nodaļās. Darba pirmā nodaļa iepazīstina ar tematu un skaidro, kas ir mākslīgais intelekts un valsts novērošana no sociālā un tehnoloģiskā skatpunkta, atklājot, kā jauno tehnoloģiju attīstība no lielajiem datiem līdz mākslīgajam intelektam ir ietekmējusi un veicinājusi masveida novērošanu. Vispirms tiek izskaidrots, ko nozīmē mākslīgais intelekts, kā tas ir saistīts ar lielajiem datiem, personas datiem un profilēšanas jēdzienu. Pēc tam tiek skaidrots novērošanas jēdziens, varas nevienlīdzība kā novērošanas pazīme, kā arī masveida novērošanas nošķiršana no mērķtiecīgas novērošanas, un apskatīts, kā jau ilgstoši valsts un sabiedrības drošība ir bijusi par pamatu dažādu masveida novērošanas pasākumu ieviešanai. Tālāk nodaļa atklāj, kādā veidā mākslīgais intelekts ir ievērojami palielinājis novērošanas praksi, un aplūko mākslīgā intelekta tehnoloģijas un metodes – sejas atpazīšanas tehnoloģijas, emociju uztveršanas tehnoloģijas (*emotion recognition technologies* – angļu val.), kā arī prognozēšanu

40 UNESCO, AHEG. (2020). Outcome document: First Draft of the Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000373434

tiesībaizsardzības nolūkos (*predictive policing* – angļu val.), kā arī atklāj, kā Covid-19 krīze ir veicinājusi digitālo novērošanas tehnoloģiju izmantošanu.

Darba otrā nodaļa apskata mākslīgā intelekta novērošanas pasākumu ietekmi uz cilvēktiesībām. Atsevišķi tiek apskatītas cilvēktiesības, kuras visvairāk ietekmē minētie pasākumi: cilvēka cieņa; tiesības uz privātumu un datu aizsardzību; diskriminācijas aizlieguma princips; bērnu tiesības; tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu; izteiksmes brīvība; pulcēšanās un biedrošanās brīvība. Grāmata apskata, kā minētās tiesības ir regulētas starptautiskajos un Eiropas cilvēktiesību dokumentos, it īpaši Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijā (ECTK)[41] un Eiropas Savienības Pamattiesību hartā (Harta)[42], kā arī Latvijas Republikas Satversmē[43], un izvērtē, kā šīs tiesības apdraud masveida novērošanas pasākumi, vienlaikus atklājot arī šo tehnoloģiju plašāku ietekmi uz sabiedrību, tiesiskumu un demokrātiskām vērtībām. Nodaļas beigās ir apskatīts pienākums ievērot cilvēktiesības krīzes situācijā, uzsverot, ka arī tādās ārkārtas situācijās, kādu radīja, piemēram, Covid-19, iedzīvotājiem nav jāizvēlas starp cilvēktiesību ievērošanu un tādu interešu aizsardzību kā sabiedrības drošība un veselība.

Grāmatas trešā nodaļa aplūko privātuma nozīmi, ko īpaši būtiski aizskar masveida novērošanas pasākumi. Lai attaisnotu aizskarošu tehnoloģiju un prettiesisku datu izmantošanu, ir bijuši daudzi mēģinājumi mazināt privātuma nozīmi, un šīm tiesībām ir veltīta plaša kritika. Nodaļā tiek atklāts, kādu labumu un aizsardzību sniedz privātums, kāpēc tas ir jāaizsargā. Apskatītas dažādas teorijas un analizēts, kāds ir tiesību uz privātumu pamatojums un nozīme, lai ierobežotu mākslīgā intelekta masveida novērošanas pasākumus. Nodaļā aplūkota tiesību uz privātumu attīstība un ka tās ietver: tiesības palikt vienam; tiesības kontrolēt informāciju par sevi; cilvēka cieņas, autonomijas un rīcības brīvības būtisku aspektu; aizsardzību pret varas ļaunprātīgu izmantošanu. Nodaļā ir aplūkota šo tiesību aizsardzība starptautiskos cilvēktiesību dokumentos un atklāts, kā tās palīdz aizsargāt arī citas cilvēktiesības, piemēram, izteiksmes un pulcēšanās brīvību. Tāpat tiek atklāts, kā privātums arvien vairāk tiek skatīts kā sabiedrības kopīga vērtība, kas kā cilvēka cieņas neatņemams elements un ētikas pamatvērtība jauno tehnoloģiju laikmetā aizsargā pret visaptverošu novērošanu un varas asimetriju, kā arī uzsvērta privātuma apzināšanās nozīme. Nodaļas nobeigumā vērsta uzmanība, ka Covid-19 pandēmijas radītā krīze ievērojami satricinājusi

41 Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija. Pieņemta 04.11.1950. (EP, Latvijā spēkā no 27.06.1997.). *Latvijas Vēstnesis*, 13.06.1997., Nr. 144/145.

42 Eiropas Savienības Pamattiesību harta. Pieņemta 07.12.2000. *OV C* 2020/239, 07.06.2016.

43 Latvijas Republikas Satversme. Pieņemta 15.02.1922. (spēkā no 07.11.1922.). *Latvijas Vēstnesis*, 01.07.1993., Nr. 43.

tiesības uz privātumu un ir steidzami nepieciešams pieņemt atbilstošus politikas pasākumus, to skaitā regulējumu, lai nepieļautu, ka masveida novērošana kļūst par jauno normu.

Grāmatas ceturtajā nodaļā ir aplūkota datu aizsardzības tiesību attīstība un mākslīgā intelekta regulējuma aizsākumi. Sākumā ir sniegts īss ieskats, kā datu aizsardzības tiesības iezīmē informācijas un komunikācijas tehnoloģiju regulējuma aizsākumu, mēģinot samērot dažāda vieda valsts un privātā sektora intereses. Nodaļas turpinājumā ir aplūkots, kā starptautiskās organizācijas – Eiropas Padome, OECD, ANO, UNESCO – ir attīstījušas datu aizsardzības tiesības, un sniegts vispārīgs pārskats, kā minētās organizācijas ir iesaistījušās diskusijā par masveida novērošanas apdraudējumu cilvēktiesībām, kā arī izvērtēts, kā šīs organizācijas ir sākušas darbu pie mākslīgā intelekta regulējuma izstrādes. Pēc tam nodaļā ir aplūkota ES datu aizsardzības regulējuma attīstība. Vispirms ir atklāts, kā pakāpeniski pieaugusi cilvēktiesību nozīme ES un kā tiesības uz datu aizsardzību Hartā atšķirībā no ECTK un citiem starptautiskajiem cilvēktiesību līgumiem tika noteiktas kā atsevišķas pamattiesības. Tiek uzsvērts, ka ES uz pamattiesībām balstītajai pieejai, kas ir pamatā datu aizsardzības regulējuma attīstībai, vajadzētu būt arī mākslīgā intelekta tehnoloģiju regulējuma turpmākās attīstības pamatā. Pēc tam ir aplūkota ES datu aizsardzības reforma un Vispārīgā datu aizsardzības regula (VDAR), kā arī speciālais datu aizsardzības regulējums, īpaši Policijas direktīva. Nodaļas beigās ir aplūkota mākslīgā regulējuma attīstība ES. Nodaļā ir atklāts, ka gan starptautiskā, gan ES līmenī arvien vairāk tiek pieprasīts skaidrs tiesiskais regulējums, kas noteiktu ierobežojumus, aizsardzības garantijas un prasības, kā arī sarkanās līnijas mākslīgā intelekta tehnoloģiju izmantošanai.

Piektā nodaļa analizē tiesību uz privātumu un datu aizsardzību ierobežošanu EST un ECT masveida novērošanas lietās. Vispirms ir īsi izskaidroti ECTK un Hartā noteiktie datu aizsardzību ierobežošanas nosacījumi. Tālāk nodaļā ir aplūkotas būtiskākās ECT lietas, kurās izvērtēta valsts novērošanas pasākumu atbilstība cilvēktiesībām, kā arī EST prakse novērošanas lietās, kas saistītas ar ES tiesību aktu spēkā esamību vai interpretāciju. Pēc tam ir detalizēti analizētas četras būtiskākās aizsardzības garantijas, kas identificētas aplūkotajās pārnacionālo tiesu lietās: skaidrs, precīzs un pieejams regulējums; samērīgums un nepieciešamība; neatkarīgs uzraudzības mehānisms; efektīvi tiesiskās aizsardzības līdzekļi. Nodaļā ir uzsvērts, ka ECT un EST praksē būtiskākais nosacījums, lai varētu veikt masveida novērošanas pasākumus, ir pienākums izvērtēt, vai šādi pasākumi ir "stingri" jeb "absolūti" nepieciešami konkrētā mērķa sasniegšanai un vai tie ir samērīgi jeb proporcionāli ar noteikto mērķi, kas ir piemērojams arī mākslīgā intelekta novērošanas pasākumiem.

Grāmatas sestā nodaļa analizē datu aizsardzības pamatprasības mākslīgā intelekta novērošanas tehnoloģijām. Aplūkoti un salīdzināti noteikumi, kas

ietverti dažādos tiesību aktos: VDAR, kas paredz vispārējās prasības, Policijas direktīvā, kas ir piemērojama attiecībā uz tiesībaizsardzības iestādēm, kā arī Konvencijā 108+. Nodaļā vispirms ir skaidrots, kas ir personas dati un biometriskie dati, aplūkoti dažādi sejas atpazīšanas tehnoloģiju izmantošanas veidi. Pēc tam analizēti personas datu apstrādes principi , kas ir pamatā un jāpiemēro, interpretējot visas pārējās datu aizsardzības prasības, – likumīgumu, nolūka ierobežojuma principu, datu minimizēšanu, precizitāti, glabāšanas ierobežojumu, datu drošību un atbildības principu. Nodaļā ir analizēta automatizēta lēmumu pieņemšana un cilvēka līdzdalības prasība, datu subjekta tiesības, kas ir piemērojamas arī attiecībā uz masveida novērošanas tehnoloģijām. Pēc tam ir aplūkota viena no visbūtiskākajām atbildības prasībām – novērtējums par ietekmi uz datu aizsardzību. Autore atklāj galvenos problēmjautājumus un regulējuma nepilnības, kas rada izaicinājumus datu aizsardzības prasību piemērošanai attiecībā uz mākslīgā intelekta novērošanas tehnoloģijām, īpašu uzmanību veltot sejas atpazīšanas tehnoloģijām. Nodaļas nobeigumā ir atsevišķi aplūkoti datu aizsardzības standarti, kas ietverti starptautisko organizāciju izdotajās rekomendācijās kontaktu izsekošanas lietotnēm, kādus izaicinājumus tie ir radījuši praksē, un vērsta uzmanība uz nepieciešamību šos standartus piemērot arī attiecībā uz mākslīgā intelekta novērošanas tehnoloģijām.

Darba pēdējā – septītā – nodaļa apkopo galvenos secinājumus un sniedz vairākus ieteikumus, kā attīstīt tālāk mākslīgā intelekta tiesisko regulējumu, kas balstās uz cilvēktiesībām un nosaka sarkanās līnijas, un kādi pārvaldības mehānismi un aizsardzības garantijas ir jāievieš praksē, lai nodrošinātu atbildīgu, uzticamu mākslīgā intelekta tehnoloģiju izmantošanu un lai aizsargātu un novērstu apdraudējumu cilvēktiesībām, demokrātijai un tiesiskumam.

1. DAĻA

Mākslīgais intelekts un valsts novērošana

Lai varētu izprast mākslīgā intelekta novērošanas tehnoloģijas un to ietekmi uz cilvēktiesībām, vispirms nodaļā ir skaidroti daži tehniskie aspekti – ko nozīmē jēdziens "mākslīgais intelekts", kā tas ir saistīts ar lielajiem datiem un personas datiem. Pēc tam aplūkots, kā mākslīgais intelekts ir ietekmējis masveida novērošanas pasākumu attīstību, kurus valsts tiesībaizsardzības iestādes ievieš drošības nolūkos. Tālāk ir aplūkotas mākslīgā intelekta novērošanas tehnoloģijas, kas šobrīd ļoti strauji attīstās – sejas atpazīšanas tehnoloģijas, emociju uztveršanas tehnoloģijas, prognozēšana tiesībaizsardzības nolūkos, kā arī dažādi digitālie novērošanas pasākumi, ko valstis ieviesa, lai cīnītos ar Covid-19 pandēmiju.

1.1. Mākslīgā intelekta, lielo datu un novērošanas izpratne

1.1.1. Mākslīgā intelekta jēdziens un izpratne

Nepastāv viena universāla mākslīgā intelekta definīcija, bet gan daudzas definīcijas, kas cenšas skaidrot mākslīgā intelekta jēdzienu. Turklāt tās attīstās līdz ar tehnoloģiju progresu.

Viena no pazīstamākajām, kā arī plašākajām mākslīgā intelekta definīcijām to skaidro kā centienus automatizēt intelektuālos uzdevumus, ko parasti veic cilvēki. Mākslīgā intelekta sistēmas darbojas ar zināmu autonomiju, lai sasniegtu iepriekš noteiktu mērķi, un šīs darbības parasti ir uzdevumi, kuriem citādi būtu nepieciešama cilvēka intelektuālo spēju izmantošana.[44]

Termins "mākslīgais intelekts" ietver nepārprotamu atsauci uz intelekta jēdzienu. Tomēr šī definīcija nav saistīta ar cilvēka intelekta aizstāšanu, bet gan ar rezultātu, ko sasniedz sistēma. Šo pieeju vislabāk izskaidro slavenais Tjūringa tests, ko Alans Tjūrings (*Alan Turing*) izvirzīja 1950. gadā. Tas apgalvo, ka mašīnu var uzskatīt par "inteliģentu", ja cilvēks, kas ar to mijiedarbojas, nevar pateikt, vai darītājs ir persona vai dators.[45] Tomēr mākslīgā intelekta sistēmas intelekts nebūt nav līdzīgs cilvēka intelektam.

Gan saistībā ar mašīnām, gan cilvēkiem "intelekts" ir neskaidrs jēdziens, kaut arī to ir ilgi pētījuši psihologi, biologi un neirozinātnieki. Tāpēc mākslīgā

44 Sk. Fjeld, et al. (2020). Principled Artificial Intelligence.

45 Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind,* 49, pp. 433–460. https://www.csee.umbc.edu/courses/471/papers/turing.pdf

intelekta pētnieki galvenokārt izmanto racionalitātes jēdzienu. Tas attiecas uz spēju izvēlēties pareizāko rīcību, lai sasniegtu noteiktu mērķi, ņemot vērā noteiktus optimizējamus kritērijus un pieejamos resursus.[46] Stjuarts Rasels (*Stuart Russell*) un Pīters Norvigs (*Peter Norvig*) definē mākslīgo intelektu kā tādu "inteliģentu aģentu" projektēšanu un veidošanu, kuri spēj uztvert apkārtējo vidi un veikt darbības, kas ietekmē šo vidi.[47] Mākslīgais intelekts vienkāršoti tiek definēts kā sistēmu spēja izmantot algoritmus, mācīties no datiem un pieņemt lēmumus līdzīgi, kā to darītu cilvēki.[48]

Eiropas Komisija mākslīgo intelektu ir ieteikusi uzskatīt par sistēmu, kas spēj demonstrēt inteliģentu rīcību, analizējot apkārtējo vidi, un ar zināmu autonomiju veikt darbības, lai sasniegtu konkrētus mērķus.[49] Šī Eiropas Komisijas definīcija ir izmantota Eiropas Parlamenta priekšlikumā Regulai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrādes, ieviešanas un izmantošanas ētikas principiem, kurā mākslīgais intelekts ir definēts kā "sistēma, kura darbojas, pamatojoties uz programmatūru, vai ir iestrādāta tehnikas ierīcēs un kuras rīcība liecina par intelektu, *inter alia* vācot, apstrādājot, analizējot un interpretējot datus par tā apkārtējo vidi un ar zināmu autonomijas pakāpi veicot darbības, ar kurām tā sasniedz konkrētus mērķus" (4. panta a) punkts).[50]

Viena no precīzākajām mākslīgā intelekta definīcijām ir sniegta Ētikas vadlīnijās uzticamam mākslīgajam intelektam, kuras 2019. gadā izstrādāja AI HLEG: "Mākslīgā intelekta (MI) sistēmas ir programmatūras (un, iespējams, arī aparatūras) sistēmas, kuras izstrādājis cilvēks un kuras, pastāvot sarežģītam mērķim, darbojas fiziski vai digitāli, uztverot apkārtējo vidi kā ievadītus datus, interpretējot savāktos strukturētos vai nestrukturētos datus, izdarot spriedumus par zināšanām vai apstrādājot no šiem datiem iegūto informāciju, kā arī pieņemot lēmumus par labāko rīcību konkrētā mērķa sasniegšanai. Mākslīgā intelekta sistēmas var izmantot simboliskus noteikumus vai mācīties

46 AI HLEG. (2019). A definition of Artificial Intelligence: main capabilities and scientific disciplines. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

47 Russel, S. J., Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*. Pearson Series in Artificial Intelligence. Hoboken: Pearson.

48 Rouhiainen, L. (2019). *Artificial Intelligence: 101 Things You Must Know Today about Our Future*, CreateSpace Independent Publishing Platform, p. 3.

49 Eiropas Komisija. (2018). Komisijas paziņojums. Mākslīgais intelekts Eiropai. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52018DC0237&from=EN

50 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru (2020/2012(INL)). https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_LV.html#title2

no cipariska modeļa, kā arī pielāgot savu darbību, analizējot, kā to iepriekšējā rīcība ir ietekmējusi vidi."[51]

Lielākā daļa mākslīgā intelekta sistēmu veic tikai daļu no definīcijā uzskaitītajām darbībām: modeļu atpazīšanu (piemēram, augu vai dzīvnieku attēlu, cilvēku sejas vai izteiksmes atpazīšana), valodu apstrādi (piemēram, runas valodu izpratne, tulkošana no vienas valodas uz citu, cīņa pret surogātpastu vai atbildēšana uz jautājumiem), praktisku ieteikumu sniegšanu (piemēram, pirkumu ieteikšana, informācijas atlase, rūpniecisko procesu optimizēšana) utt. Tajā pašā laikā dažas sistēmas var apvienot daudzas šādas spējas, piemēram, pašvadāmie transportlīdzekļi vai militārie un aprūpes roboti.[52] Mākslīgā intelekta sistēmas var būt gan tīri programmatiskas, piemēram, virtuālie asistenti, attēlu analīzes sistēmas, meklētājprogrammas, runas un sejas atpazīšanas sistēmas, gan arī aparatūrā ietvertas sistēmas, piemēram, robotos, pašbraucošās automašīnās, dronos un lietu internetā.

AI HLEG mākslīgo intelektu kā zinātnes disciplīnu apraksta šādi: "Mākslīgais intelekts kā zinātnes disciplīna ietver dažādas pieejas un paņēmienus, piemēram, mašīnu mācīšanos (konkrēti piemēri – mašīnu dziļā mācīšanās un stimulētā mācīšanās), mašīnu spriešanu (ietver plānošanu, programmu veidošanu, zināšanu reprezentāciju un spriešanu, meklēšanu un optimizēšanu) un robotiku (ietver kontroli, uztveri, sensorus un iedarbinātājus, kā arī pārējo paņēmienu integrēšanu kiberfiziskās sistēmās)."[53]

Mākslīgais intelekts ir vispārīga joma, kas ietver mašīnmācīšanos un dziļo mācīšanos, taču tajā ietilpst arī daudz citu darbību, kas neiekļauj mācīšanos. Piemēram, agrīnās šaha programmas izmanto tikai stingri kodētus noteikumus.

Patlaban mākslīgā intelekta galvenie virzieni ir: problēmu risināšana (piemēram, plānošana un meklēšana), zināšanu un pamatojuma izstrāde (attiecas uz lēmumu pieņemšanu), mašīnmācīšanās (ietver dziļo mācīšanos, neironu tīklus), mijiedarbība (piemēram, robotika, cilvēka aģenta un robota mijiedarbība), dabiskās valodas apstrāde (tulkošana, informācijas iegūšana), uztveres attīstīšana (redzes spējas un attēla atpazīšana).[54]

Mašīnmācīšanās ir viens no primārajiem mākslīgā intelekta virzieniem. Tā ir datu analīzes metode, kas izmanto mācību algoritmus, lai automatizēti atklātu

51 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

52 Sk. Sartor, G., Lagioia, F. (2020). The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence. European Parliament. http://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

53 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

54 François, C., Allaire, J. J. (2018). *Deep Learning with R*. Shelter Island, NY: Manning Publications Co, p. 4. Sk. Dignum, V. (2019). *Responsible Artificial Intelligence. How to Develop and Use AI in a Responsible Way*. Springer, p. 12.

modeļus lielās datu kopās, ģenerētu modeļus un izmantotu tos prognozēm. Mašīnmācīšanās sistēmas tiek apmācītas, nevis tieši programmētas.[55] Tām ir iespēja mācīties no tā, kā tiek izmantotas, lai tās spētu piedāvāt personalizētu lietotāja pieredzi. Viens no zināmākajiem piemēriem ir personalizēšana, ko varam redzēt, piemēram, "Meta" ("Facebook") un citās sociālo mediju platformās un "Google" meklētājprogrammas rezultātos.

Viens no straujāk augošajiem mākslīgā intelekta novirzieniem ir dziļā mācīšanās, kas ir mašīnmācīšanās apakšnozare. Dziļā mācīšanās izmanto vairāku slāņu neironu tīklus, lai atpazītu sarežģītas attiecības un modeļus datos. Dziļās mācīšanās algoritmi var atpazīt un kategorizēt informāciju un identificēt modeļus. Tas ļauj mākslīgā intelekta sistēmām nepārtraukti mācīties darbībā un uzlabot rezultātu kvalitāti un precizitāti, nosakot, vai lēmumi ir pareizi.[56]

Mākslīgie neironu tīkli, kurus bieži dēvē vienkārši par neironu tīkliem, savu nosaukumu ir guvuši, iedvesmojoties no bioloģiskajiem neironu tīkliem, lai gan tie darbojas ļoti atšķirīgi. Neironu tīklam ir ievade – dati, kas nāk no sensoriem, un izvade – attēla interpretācija. Tīkla apmācības posmā, analizējot piemērus, savienojumu svarīgums tiek pielāgots, lai pēc iespējas vairāk atbilstu pieejamiem piemēriem, tas ir, lai samazinātu kļūdu starp paredzamo un tīkla aprēķināto izvadi. Apmācības posma beigās notiek neironu tīkla rīcības testēšanas fāze, kurā, izmantojot iepriekš neredzētus piemērus, tiek pārbaudīts, vai uzdevums ir labi iemācīts.[57] Ir svarīgi ņemt vērā, ka šai pieejai, tāpat kā visām mašīnmācīšanās metodēm, vienmēr ir noteikts kļūdas procents, lai arī tas parasti ir mazs. Tāpēc svarīgs faktors ir precizitāte, pareizo atbilžu procentuālā attiecība.

Mākslīgā intelekta sistēmas tiek apmācītas, balstoties uz ārējās pasaules datiem vai arī cilvēka veidotās vides apmācāmajiem datiem, tādējādi pieņemtie lēmumi un to kvalitāte kļūst tieši atkarīga no šo datu avota, kvalitātes un objektivitātes. Dziļo mašīnmācīšanās metožu algoritmiskie rezultāti ir grūti interpretējami, kā rezultātā šo mākslīgā intelekta sistēmu pieņemtie lēmumi var nebūt izskaidrojami. Proti, neviens nevar pateikt, kādēļ lēmumi ir tieši tādi un ne citādi.[58]

55 François, C., Allaire, J. J. (2018). *Deep Learning with R*. Shelter Island, NY: Manning Publications Co, p. 4. Sk. Dignum, V. (2019). *Responsible Artificial Intelligence. How to Develop and Use AI in a Responsible Way*. Springer, p. 5.

56 Sk. François, Allaire (2018), *Deep Learning with R*, pp. 8–11; Dignum (2019), *Responsible Artificial Intelligence*, pp. 27–28.

57 AI HLEG. (2019). A definition of Artificial Intelligence.

58 Sk. Barredo Arrieta, Díaz-Rodríguez, N., Del Ser, J. et al. (2020). Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI. *Information Fusion,* 58, pp. 82–115. https://doi.org/10.1016/j.inffus.2019.12.012; VARAM. (2020). Informatīvais ziņojums "Par mākslīgā intelekta risinājumu attīstību". https://www.varam.gov.lv/lv/jauns-informativais-zinojums-par-maksliga-intelekta-risinajumu-attistibu

Ir jānošķir šobrīd esošās mākslīgā intelekta iespējas no nākotnes iespējām. Visattīstītākā mākslīgā intelekta sistēma vēl joprojām ir t. s. šaurais mākslīgais intelekts, kas izstrādāts, lai risinātu konkrētus uzdevumus vai problēmas. Šaurais mākslīgais intelekts tiek pretstatīts vispārīgam mākslīgam intelektam. Ja tiktu izstrādāts vispārīgs mākslīgais intelekts, autonomās mašīnas kļūtu spējīgas uz vispārīgu saprātīgu darbību un varētu veikt plašu uzdevumu klāstu. Tāpat kā cilvēki tas būtu spējīgs vispārināti un abstrakti mācīties, izmantojot dažādas kognitīvās funkcijas, tam būtu asociatīvā atmiņa, un tas spētu spriest un pieņemt lēmumus.[59] Pašreiz mēs varam runāt par vispārīgo mākslīgo intelektu tikai kā par hipotētisku attīstības iespēju tālākā nākotnē. Lai gan tādu mākslīgo intelektu varam redzēt vienīgi zinātniskās fantastikas filmās un grāmatās un mums nav jābaidās no robotiem, kas pārņems pasauli, tajā pašā laikā mākslīgais intelekts pēdējo gadu laikā attīstās zibens ātrumā un jau šobrīd rada ne tikai daudz ieguvumu dažādās jomās, piemēram, izglītības, veselības, vides, transporta jomā, bet var arī radīt būtiskus apdraudējumus sabiedrībai, kurus ir nepieciešams novērst.

Kaut arī mākslīgais intelekts kā zinātnes disciplīna ir pastāvējis jau kopš 20. gadsimta 50. gadiem, tikai nesen tas kļuvis par vispārzināmu jēdzienu. Var rasties jautājums, kāpēc mākslīgais intelekts tieši pēdējos gados ir kļuvis tik populārs. Tā straujo attīstību ir ietekmējuši trīs būtiski aspekti. Pirmkārt, pēdējo gadu laikā ir izdevies savākt agrāk nepieredzētu milzīgu datu daudzumu. Otrkārt, tiek izstrādāti arvien efektīvāki algoritmi. Treškārt, ir kļuvusi pieejama ļoti liela skaitļošanas jauda. Šo trīs elementu apvienojums ir ļāvis mākslīgajam intelektam ļoti strauji attīstīties. Vienkāršoti, mākslīgo intelektu var dēvēt par tehnoloģiju kopumu, kas apvieno datus, algoritmus un datošanas jaudu.[60] Mākslīgā intelekta sadalīšana šajos trīs pamatelementos ļauj labāk uztvert saistību starp mākslīgo intelektu un citiem jēdzieniem, kas iepriekš jau izraisījuši politikas izmaiņas un diskusijas šajā jomā. Viens no tādiem ir lielie dati.

1.1.2. Mākslīgais intelekts un lielie dati

Pašlaik viena no galvenajām politiskajām prioritātēm ir mākslīgais intelekts un tā regulējuma izstrāde, bet agrāk plašas diskusijas un daudzi regulējuma priekšlikumi bija saistīti ar lielajiem datiem un to radītajiem izaicinājumiem, it īpaši datu aizsardzībai.

Lielie dati būtiski maina veidu, kādā informācija tiek vākta, apvienota un analizēta. Lielie dati, kas galvenokārt balstās uz mijiedarbību ar citu tehnoloģisko vidi, piemēram, lietu internetu un mākoņdatošanu, var sniegt nozīmīgu labumu

59 OECD. (2017). OECD Digital Economy Outlook 2017. https://doi.org/10.1787/9789264276284-en

60 Eiropas Komisija (2020), Baltā grāmata par mākslīgo intelektu.

un inovācijas sabiedrībai, uzlabojot biznesa produktivitāti, valsts sektora darbību, kā arī sabiedrības līdzdalību. Lielie dati var sniegt vērtīgu informāciju, kas ļauj saprast un pārvaldīt sabiedrību.

Pastāv daudzas lielo datu definīcijas, kas atšķiras atkarībā no konkrētās disciplīnas. Lielākā daļa no tām koncentrējas uz pieaugošo tehnoloģisko spēju savākt, apstrādāt un iegūt jaunas un paredzamas zināšanas no liela apjoma datiem, to ieguves ātruma un daudzveidības. Termins "lielie dati" parasti apzīmē ārkārtīgi lielas datu kopas, kuras var aprēķināt skaitliski, lai iegūtu secinājumus par datu modeļiem, tendencēm un korelācijām. Kā norāda Starptautiskā telekomunikāciju savienība, lielie dati ir "paradigma, kas ļauj apkopot, uzglabāt, pārvaldīt, analizēt un vizualizēt, iespējams, ar reāllaika ierobežojumiem, plašu datu kopu ar neviendabīgām īpašībām".[61]

Definīcija "lielie dati" ietver lielo datu analīzi.[62] Galvenie jautājumi, kas saistīti ar datu aizsardzību, attiecas ne tikai uz apstrādāto datu apjomu, ātrumu un daudzveidību, bet arī uz datu analīzi, izmantojot programmatūru, lai iegūtu jaunas un paredzamas zināšanas lēmumu pieņemšanai par personām un personu grupām.[63]

Mākslīgā intelekta sistēmu izstrāde, kas balstīta uz mašīnmācīšanos, veicina milzīgu datu kopu – lielo datu – izveidi. Lai mākslīgais intelekts varētu mācīties, tam ir nepieciešams milzīgs datu apjoms, ko analizēt, un tas pieprasa arvien vairāk datu.

Tajā pašā laikā digitalizācija ir notikusi pirms lielākās daļas mākslīgā intelekta sistēmu izveides. Datu plūsmas tiek veidotas visur, kur tiek izmantota skaitļošana. Mūsu digitālās pasaules pamatā ir nepārtraukta datu plūsma. Katru sekundi milzīgus datu apjomus iegūst un apstrādā daudz un dažāda veida sistēmas un ierīces, piemēram, sistēmas, kuras izmanto, lai veiktu ekonomiskos darījumus (piemēram, e-komercijā); sensori, kas uzrauga un nodrošina fizisko objektu darbību (piemēram, transportlīdzekļos vai viedo māju ierīcēs); darbplūsmas, ko rada ekonomiskas un valdības darbības (piemēram, banku, transporta vai nodokļu jomā);

61 ITU. (2015). Recommendation Y.3600. Big data – Cloud computing based requirements and capabilities. https://www.itu.int/rec/T-REC-Y.3600-201511-I/en

62 Terminu "lielo datu analīze" lieto, lai identificētu skaitļošanas tehnoloģijas, kas analizē lielu datu apjomu ar mērķi atklāt slēptos modeļus, tendences un korelācijas. Eiropas Savienības Kiberdrošības aģentūra skaidro, ka termins "lielo datu analītika" attiecas uz visu datu pārvaldības dzīves ciklu, kurā tiek vākti, organizēti un analizēti dati, lai atklātu modeļus, secinātu situācijas vai stāvokļus, prognozētu un izprastu uzvedību. Sk. arī ENISA. (2015). Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. https://www.enisa.europa.eu/publications/big-data-protection

63 Council of Europe. (2017). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (T-PD). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. https://rm.coe.int/16806ebe7a

novērošanas ierīces (piemēram, videokameras satiksmes kontrolei vai piekļuves kontroles sistēmas); sistēmas, ko izmanto nekomerciālām darbībām (piemēram, piekļuve internetam, meklēšana vai sociālie tīkli) utt.

Informācijas un datu apjoms pasaulē turpina pieaugt neiedomājami strauji. Pēdējo gadu laikā šīs datu plūsmas ir integrētas globālā savienotā datu apstrādes infrastruktūrā, kuras centrā ir internets. Šī infrastruktūra ir universāls līdzeklis saziņai, piekļuvei datiem un jebkura veida privātu un sabiedrisku pakalpojumu sniegšanai. Tā ļauj iedzīvotājiem iepirkties, izmantot banku un citus pakalpojumus, maksāt nodokļus, saņemt valsts pabalstus un tiesības, piekļūt informācijai un zināšanām, kā arī veidot sociālos kontaktus.

Digitālās pēdas atstāj gandrīz katra mūsu ikdienas darbība – ikviena dalīšanās ar ziņu vai "patīk" nospiešana, ziņas vai fotogrāfijas aplūkošana "Facebook", "Linkedin", "Twitter", "Instagram", katrs nosūtītais e-pasts vai ziņa koplietošanas platformās, meklēšana internetā, iepirkšanās "Amazon", mūzikas klausīšanās "Spotify", filmas skatīšanās "Netflix", skriešana vai pastaiga laukā, ja līdzi ir fitnesa aproce vai mobilais telefons, kurā ir instalētas lietotnes, kas vāc atrašanās vietas datus.

Datu apjoms, kas tiek radīts internetā pasaulē katru minūti, ir šokējoši liels. 2020. gadā ikvienu minūti "Google" tiek veikti vairāk nekā 4 miljoni meklējumu, "YouTube" skatīti 4,7 miljoni video, "WhatsApp" un "Facebook Masanger" nosūtīti 59 miljoni ziņu, kā arī nosūtīti 190 miljoni e-pasta vēstuļu. Turklāt ar katru gadu radīto datu apjoms strauji palielinās.[64]

Mobilo un interneta pakalpojumu un piekļuves ieviešana ir būtiski mainījusi datu vākšanas, analīzes un izmantošanas raksturu. 21. gadsimtā dati kļūs par lielāko vērtību, par ko sacenšas gan privātās kompānijas, gan valsts iestādes. Ikviens vēlas kontrolēt šo datu plūsmu, jo tā sniedz varu.

Lielie tehnoloģiju uzņēmumi, piemēram, "Google", "Meta" ("Facebook") un "Apple", sacenšas par to, lai piesaistītu mūsu uzmanību arvien vairāk, ne tikai lai varētu pārdot reklāmas, bet arī lai iegūtu arvien lielāku datu daudzumu. Šie interneta tehnoloģiju milži ir izveidojuši tā saukto uzmanības ekonomiku, kur galvenā prece ir cilvēka uzmanība. Digitālā joma ir veidota tā, lai cilvēki atdotu savu vērtīgo laika, uzmanības un datu resursus, neņemot vērā izmaksas, ko tas rada šīm personām un citiem.[65] Dati nav vērtība tikai tāpēc, ka tos var pārdot. Tehniski ne

64 Aystin, D. (16 April, 2021). Here is Your 2021 Internet Minute Infographic!: eDiscovery Trends. *eDiscoveryToday.* https://ediscoverytoday.com/2021/04/16/here-is-your-2021-internet-minute-infographic-ediscovery-trends/

65 Lewandowsky, S., Smillie, L., Garcia, D. et al. (2020). Technology and Democracy: Understanding the influence of online technologies on political behaviour and decision-making. Publications Office of the European Union, Luxembourg. https://data.europa.eu/doi/10.2760/709177

"Facebook", ne "Google" nepārdod datus, bet gan varu ietekmēt. Tie vāc, saglabā un analizē datus, lai varētu pārdot varu – varu parādīt reklāmas, varu piesaistīt uzmanību, varu ietekmēt uzvedību. "Google" un "Facebook" tikai tehniski nodarbojas ar datu biznesu, pamatā tas ir varas bizness. Personas dati pat vairāk nekā naudas pieaugums piešķir varu tiem, kas tos vāc un analizē, un tieši šī vara mūsu datus padara tik iekārojamus.[66]

Datu daudzums, ko mēs saražojam, turpinās palielināties, strauji pieaugot lietu internetam – visu veidu ierīcēm, sensoriem un mašīnām, kas ir savienotas un savstarpēji sazinās. Globālā savstarpēji saistītā datu apstrādes infrastruktūra ietver aptuveni 30 miljardus ierīču – datorus, viedtālruņus, mašīnas, kameras utt. –, kas ģenerē milzīgus datu apjomus.[67]

Ne visi dati, kas tiek apstrādāti lielo datu kontekstā, ir personas dati un saistīti ar mijiedarbību ar cilvēkiem, taču liela daļa attiecas uz tiem, tieši ietekmējot personas un viņu tiesības attiecībā uz personas datu apstrādi. Turklāt, tā kā lielie dati ļauj savākt un analizēt lielu datu apjomu, lai identificētu attieksmes modeļus un prognozētu grupu un kopienu uzvedību, ir jāņem vērā arī tas, ka ar datu izmantošanu saistītajiem riskiem ir kolektīva dimensija.[68]

Mākslīgā intelekta tehnoloģijas palielina datu apstrādes spējas veikt lielo datu analīzi un datu sasaisti un ir būtiski mainījušas datu vākšanas, analīzes un izmantošanas raksturu. Pateicoties mākslīgā intelekta metožu, milzīgā datu apjoma un skaitļošanas jaudas kombinācijai, ir kļuvis iespējams automātiski prognozēt un novērtējumus balstīt uz daudz vairāk piemēriem, ņemot vērā daudz lielāku skaitu katram no tiem piemītošu pazīmju jeb īpašību kopumu, lai panāktu daudz augstāku precizitātes līmeni. Tas tiek izmantots dažādiem mērķiem, piemēram, mērķorientētai reklāmai, kas balstīta uz ierakstiem par patērētāja īpašībām un uzvedību, piemēram, dzimumu, vecumu, pirkumu vēsturi.

Personas var pakļaut novērošanai un ietekmei dažādos veidos un kontekstos, balstoties uz plašu personisko īpašību kopumu, sākot no ekonomiskiem apstākļiem, veselības situācijas, dzīvesvietas, personiskās dzīves izvēlēm un notikumiem, uzvedības utt. Ar atbilstošām klasifikācijas un prognozēšanas metodēm analizējot un salīdzinot datus par personām, mākslīgais intelekts palielina profilēšanas iespējas, un tas ļauj izsecināt informāciju par šīm personām vai grupām un uz tā pamata veikt novērtējumu un pieņemt lēmumus.

66 Véliz, C. (2021). *Privacy Is Power: Why and How You Should Take Back Control of Your Data.* Bantam Press, p. 49.

67 Statista. (2019). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

68 Sk. Council of Europe (2017), Consultative Committee of the Convention for the Protection .. (T-PD).

Termins "profils" ir cēlies no itāļu valodas vārda *profilo*, kas nāk no *profilare* un sākotnēji nozīmē 'vilkt līnijas', it īpaši objekta kontūras. Tieši tā ir profilēšanas ideja, izmantojot datu apstrādi, respektīvi, paplašināt pieejamos datus par dažādu grupu indivīdiem, lai ieskicētu (aprakstītu vai paredzētu) viņu iezīmes un tieksmes.[69] Profilēšanas radītos draudus varēja spilgti redzēt "Cambridge Analytica" lietā, kas saistīta ar mēģinājumiem ietekmēt balsotāju rīcību ASV 2016. gada vēlēšanās, pamatojoties uz masveida personas datu apstrādi.[70]

Patlaban nostiprinās pastāvīga, uz datiem balstīta prognozēšanas pasaule, kurā mēs, iespējams, vairs nespēsim izskaidrot lēmumu iemeslus, un tas rada daudzus jaunus riskus un apdraudējumus. Arvien vairāk lēmumu cilvēku vietā pieņem algoritmi, kurus turklāt mēs nesaprotam. Lielo datu algoritmu novērošana attiecas uz visiem, jo tie fiksē un analizē katru darbību internetā. Mēs arvien vairāk paļaujamies uz lielo datu algoritmiem, piemēram, "Google" meklēšanas rezultātiem, "Google Map" maršrutiem, "Amazon" ieteikumiem, ko pirkt, "YouTube" ieteikumiem, ko klausīties, "Netflix" ieteikumiem, ko skatīties, utt. Platformas izmanto "ieteikumu" sistēmas, lai atlasītu to, kas katram ir visatbilstošākais – nākamais videoklips, ko mēs skatāmies, nākamais nopērkamais produkts, nākamais viedoklis vai jaunumi mūsu sociālo mediju ziņu plūsmas augšdaļā. Algoritmi nosaka, kādas grāmatas mums lasīt, kādas filmas skatīties, kādu mūziku klausīties, pa kādu maršrutu braukt, kur dzīvot, uz kurieni braukt atpūsties, kur mācīties, ar ko satikties utt. Ir grūti saprast, kā tie pieņem lēmumus un vai tie sniedz precīzu priekšstatu par pasauli. Arvien biežāk uzticamies algoritmiem, taču nesaprotam to pieņemtos lēmumus un arvien vairāk kļūstam kā marionetes šo algoritmu rokās. Šiem algoritmiem var būt arī nopietna ietekme uz mūsu autonomiju, nosakot to, kā redzam apkārtējo pasauli. Spēja pašiem pieņemt lēmumus ir būtisks cilvēka autonomijas aspekts, ko mēs pakāpeniski zaudējam. Arvien lielāka paļaušanās uz algoritmiem rada neapturamu tendenci, ka cilvēki arvien vairāk tiek pakļauti lēmumiem, ko pieņēmušas mākslīgā intelekta sistēmas vai kas pieņemti ar to palīdzību. Turklāt šie lēmumi var būt grūti saprotami un apstrīdami, un dažkārt tie var ļoti būtiski ietekmēt cilvēka dzīvi.

Mākslīgā intelekta sistēmas tiek izmantotas, ne tikai lai ietekmētu lietotāju un patērētāju rīcību un izvēles, bet tās arvien vairāk lieto gan privātie uzņēmumi, gan valsts iestādes, lai pieņemtu lēmumus, kas skar personas un kam var būt būtiska ietekme. Arvien vairāk algoritmisko lēmumu pieņemšanas sistēmas tiek izmantotas lēmumu pieņemšanas atbalstam. Daudzās situācijās šādu lēmumu ietekme var būt ļoti nozīmīga, piemēram, ja tas ir saistīts ar izglītību, nodarbinātību,

69 Sk. Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

70 Sk. EDPS. (2018). Opinion 3/2018. EDPS Opinion on online manipulation and personal data. https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

veselības aizsardzību, kredīta piešķiršanu, soda noteikšanu un tiesas spriedumiem. Algoritmu prognozes var tikt izmantotas, lai pieņemtu dažāda veida lēmumus, piemēram, klienta kredītspējas noteikšanai, darba pieteikumu izvērtēšanai un pat lai noteiktu, kādu atzīmi skolēns saņems vidusskolas gala eksāmenā.[71] Tiesībaizsardzības iestādes var izmantot tos, lai prognozētu, vai persona izdarīs noziedzīgu nodarījumu un uz tā pamata būtu arestējama, kaut gan šīs prognozes var būt kļūdainas un diskriminējošas.

Liela daļa problēmu ir saistītas ar inteliģento mašīnu spēju vai, precīzāk, spējas trūkumu pieņemt ētiskus lēmumus un lēmumu pieņemšanas procesā ņemt vērā cilvēciskās vērtības un ētiskos principus. Viens no lielākajiem izaicinājumiem ir, kā nodrošināt, ka algoritmisko lēmumu pieņemšanas sistēmas būtu taisnīgas. Tās var būt diskriminējošas dažāda veida aizspriedumu dēļ, kas izriet no apmācības datiem, tehniskiem ierobežojumiem vai arī sabiedrības vai individuāliem aizspriedumiem. Vairākumā gadījumu rezultāts būs netaisnīgs un diskriminējošs tad, ja tas nesamērīgi ietekmē noteiktas grupas bez pieņemama pamatojuma. Šādas sistēmas var radīt un veicināt aizspriedumus pret noteiktas grupas locekļiem, ja uz šo grupu attiecas tikai ļoti maza daļa no apmācāmajiem datiem, jo tas samazina paredzamības precizitāti attiecībā uz šo grupu. Piemēram, sejas atpazīšanas algoritmi, kas tiek izstrādāti, pamatā izmantojot baltādainu vīriešu fotoattēlus, būs daudz mazāk precīzi un to piemērošana būs diskriminējoša pret sievietēm un citas etniskās piederības cilvēkiem.

Viena no mākslīgā intelekta attīstības tendencēm, kas šobrīd ļoti strauji attīstās un var radīt būtisku apdraudējumu cilvēktiesībām, ir masveida novērošanas tehnoloģijas, it īpaši sejas atpazīšanas un citas biometriskās tehnoloģijas. Tomēr, pirms analizējam konkrētas mākslīgā intelekta tehnoloģijas un to radītos riskus, īsumā apskatīsim, ko nozīmē novērošana un kā tā ir attīstījusies līdz mūsdienu datu un mākslīgā intelekta laikmetam.

1.1.3. Digitālās masveida novērošanas attīstība

1.1.3.1. Novērošanas jēdziens

Novērošanas jēdzienam pašam par sevi ir gara vēsture tiesiskuma, tiesībaizsardzības un izlūkošanas zinātniskajās un filozofiskajās diskusijās. Kaut arī novērošanas (*surveillance* – angļu val.) definīcijas atšķiras, lielākā daļa zinātnieku uzsver, ka tā ir kas vairāk nekā tikai skatīšanās, tā ir atkarīga arī no spējas kontrolēt,

71 Mayer-Schonberger, V., Cukier, K. (2017). *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight*. London: John Murray, p. 17.

regulēt vai ietekmēt uzvedību.[72] Vārds "novērošana" ir cēlies no franču valodas vārda *surveillance*, kas nozīmē 'skatīties pāri' jeb 'skatīties no augšas'.[73] Etimoloģiski tas izriet no latiņu valodas vārda *vigilare*, kas nozīmē 'uzraudzīt', 'apsargāt', 'skatīties'.[74] Tas nenozīmē tikai pasīvu skatīšanos vai novērošanu, bet gan pārraudzību, kas veikta ar mērķi pieņemt kādus lēmumus un iejaukties, lai mainītu uzvedību.

Termina "novērošana" vietā var arī lietot vārdu "uzraudzība"[75], kas arī atspoguļo šo darbību mērķi "kontrolēt" vai "regulēt" sabiedrību. Ar terminu "uzraudzība" tiesībaizsardzības kontekstā tiek saprasta cilvēku vai grupu novērošana, kas veikta, izmantojot personas datu sistēmas, lai regulētu vai vadītu viņu uzvedību.[76] Turklāt, lai tā būtu efektīva, nav nepieciešams, lai cilvēki zinātu par šādas uzraudzības veikšanu, gluži pretēji – slepenai uzraudzībai pat ir lielāks spēks. Tajā pašā laikā vārds "uzraudzība" tiek lietots ļoti dažādos kontekstos, piemēram, uzraudzības mehānismi un uzraudzības iestādes. Sabiedrībā plašāk lietots ir termins "novērošana", piemēram, visiem zināmas ir videonovērošanas tehnoloģijas. Tāpēc grāmatā pamatā tiek lietots jēdziens "novērošana", bet atkarībā no konteksta dažkārt darbā var tikt izmantots arī otrs jēdziens.

Var izšķirt dažādus novērošanas veidus. 1971. gadā Alans Vestins (*Alan Westin*) darbā "Informācijas tehnoloģijas demokrātijā" identificēja trīs novērošanas formas, ko var izmantot valsts iestāde: fiziskā, psiholoģiskā un datu. Fiziskā novērošana ietver personas fizisku novērošanu vai noklausīšanos, psiholoģiskā – ietver nopratināšanas formas, kā arī personības testus, ko izmanto darba devēji, savukārt datu novērošana ietver informācijas atklāšanu, kas notiek, veicot ikvienu darbību, tās vākšanu un saglabāšanu.[77] Tomēr par datu novērošanu nevar uzskatīt ikvienu datu apstrādes procesu.

Datu novērošana ir attiecināma uz datu apstrādi un izmantošanu sistēmās, kas galvenokārt saistītas ar novērošanas veikšanu, bet ne uz tādu apstrādi, kurai

72 Monahan, T., Wood, D. M. (2018). Introduction. Surveillance Studies as a Transdisciplinary Endeavor. In: Monahan, T., Wood, D. M. (eds.), *Surveillance Studies: A Reader*. New York: Oxford University Press.

73 Ibid.

74 Moore, P. V. (2020). *Data subjects, digital surveillance, AI and the future of work*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf

75 No angļu valodas vārdu "*surveillance*" var tulkot gan kā 'uzraudzība', gan 'novērošana'.

76 Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the ACM* 31(5), 498–512. Sk. Ferguson, A. G. (2017). Big data Surveillance: The Convergence of Big data and Law Enfocement, p. 171. In: Gray, D., Henderson, S. E. (eds), *The Cambridge Handbook on Surveillance Law.* Cambridge University Press, pp. 171–197.

77 Lloyd, I. J. (2020). *Information Technology Law*. 9th ed. Oxford: Oxford University Press, pp. 11–12.

ir citi mērķi.[78] Vienlaikus jāpatur prātā, ka sākotnējie sistēmas izmantošanas mērķi var tikt mainīti un arī jau pieejamie dati vēlāk var tikt izmantoti novērošanas sistēmās, piemēram, fotogrāfiju datubāzes var izmantot sejas atpazīšanas sistēmu izstrādē.

Līdz ar tehnoloģiju, datu vākšanas, glabāšanas un analīzes metožu attīstību datu novērošana ir kļuvusi par galveno un izplatītāko novērošanas veidu, ko izmanto gan valsts un tiesībaizsardzības iestādes, gan privātie uzņēmumi dažādu savu interešu vārdā. To var dēvēt arī par digitālo vai elektronisko novērošanu, kas ietver dažādus veidus: audio, vizuālo, metadatu, komunikācijas, biometrisko novērošanu jeb uzraudzību. Turklāt robežas starp dažādām novērošanas formām izzūd, piemēram, fiziskā novērošana var notikt, izmantojot lokalizācijas datus, kā arī videonovērošanas kameras.

Sākotnēji novērošanu veica valsts tiesībaizsardzības iestādes, savukārt tagad to arvien plašāk izmanto privātie uzņēmumi. Dati un tehnoloģijas ir būtiskais faktors, kas veicinājis valsts iestāžu kontroli jeb varu pār iedzīvotājiem, kā arī lielo tehnoloģiju uzņēmumu kontroli pār lietotājiem.

1.1.3.2. Varas nevienlīdzība kā novērošanas pazīme

Veicot novērošanu, vienmēr pastāv varas nevienlīdzība. Privātā sektorā pastāv nevienlīdzīgas pozīcijas starp lielajiem tehnoloģiju un sociālo mediju uzņēmumiem un lietotājiem. Uzmanības resursi ir ierobežoti, bet pieprasījums pēc informācijas algoritmiskai apstrādei strauji aug. Tas ir radījis ļoti asimetriskas attiecības starp sociālo mediju platformām un to lietotājiem. Platformām ir dziļas zināšanas par lietotāja uzvedību un pat intīmiem dzīves aspektiem, savukārt lietotāji maz zina par to, kā tiek vākti viņu dati, kā tie tiek izmantoti komerciāliem vai politiskiem mērķiem un kā šie dati tiek izmantoti, lai veidotu lietotāju tiešsaistes pieredzi. Šī zināšanu asimetrija izpaužas arī kā varas asimetrija.

Zināt par citiem, vienlaikus maz atklājot par sevi, ir vissvarīgākais komerciālās varas veids uzmanības ekonomikā jeb ekonomikā, ko nosaka patērētāju uzmanība. Novērot citus, vienlaikus izvairoties, lai paši netiktu novēroti, ir arī galvenā autoritārās politiskās varas pazīme.[79] Š. Zubofa norāda, ka valsts īstenotas novērošanas apvienojums ar kapitālisma sistēmā veiktu novērošanu nozīmē, ka digitālās tehnoloģijas visu sabiedrību sadala divās grupās: vērotāji (neredzami,

78 Gstrein, O. J. (2020). Mapping Power and Jurisdiction on the Internet through the Lens of Government-Led Surveillance. *Internet Policy Review*, 9(3). https://doi.org/10.14763/2020.3.1497

79 Lewandowsky, Smillie, Garcia, et al. (2020), Technology and Democracy.

nezināmi un bez atbildības) un vērojamie. Zināšanu asimetrija nozīmē varas asimetriju, kam savukārt ir dziļas sekas uz demokrātiju.[80]

Varas nevienlīdzība izpaužas daudzās jomās. Nevienlīdzīgās pozīcijās atrodas darbinieki un darba devējs, kurš tos novēro, piemēram, izsekodams darbinieku datorus, izmantojot videonovērošanu vai pat emociju uztveršanas tehnoloģijas darbavietā. Nevienlīdzīgas attiecības pastāv arī starp iedzīvotājiem, kurus novēro, un valsti, kas veic dažādus novērošanas pasākumus tādu sabiedrībai nozīmīgu interešu vārdā kā drošība, un tie bieži vien ir slepeni, iedzīvotāji netiek par tiem informēti.

Valsts novērošana vienmēr ir bijusi atzīta par daļu no valsts suverenitātes īstenošanas. Novērošana ir viens no galvenajiem instrumentiem cīņā pret terorismu, un tai ir būtiska nozīme izlūkošanas pasākumu veikšanā, lai novērstu teroraktus un aizturētu teroristus. Bet, kā spilgti parādīja 2013. gada Edvarda Snoudena atklājumi, šīs darbības var arī būtiski ierobežot pamattiesības, it īpaši privātumu un datu aizsardzību.

Visai pasaulei ļoti liels pārsteigums bija ASV Nacionālās drošības aģentūras (NSA) bijušā darbinieka Edvarda Snoudena atklājumi par ASV īstenoto slepeno masveida elektroniskās novērošanas programmu, kas bija saistīta gan ar ASV pilsoņu, gan citu valstu personu telekomunikācijas un datu plūsmas novērošanu iepriekš neiedomājamos apmēros. 2013. gadā žurnālos "The Guardian"[81] un "The Washington Post" tika publicēti raksti, kas atklāja, ka ASV darbojas slepena masveida elektroniskās novērošanas programma, kura ļauj piekļūt ASV vadošo interneta uzņēmumu, tostarp "Microsoft", "Yahoo", "Google", "Facebook", "Skype", "YouTube", "Apple", interneta datiem, piemēram, e-pastiem, nosūtītajām ziņām, video, fotoattēliem, pārsūtītajiem failiem, darbībām sociālajos tīklos. Tika atklāts, ka NSA un ASV Federālais izmeklēšanas birojs pieslēdzās tieši šo interneta uzņēmumu serveriem, lai izsekotu tiešsaistes saziņu uzraudzības programmas ietvaros, kas zināma kā PRISM. Turklāt tie atklāja plašu datu apmaiņu starp tā saukto "Five Eyes" izlūkošanas tīklu, kurā ietilpst Lielbritānija, ASV, Austrālija, Kanāda un Jaunzēlande un kurā dominē NSA, kā arī plašu sadarbību starp

80 Zuboff (2019), *The Age of Surveillance Capitalism*, pp. 188–189, 281; Naughton (20 January, 2019), 'The goal is to automate us'.

81 Sk. Greenwald, G., MacAskill, E. (7 June, 2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian.* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; Ackerman, S., Rushe, D. (3 February, 2014). The Microsoft, Facebook, Google and Yahoo release US surveillance requests. *The Guardian*. http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests

dažādu ES dalībvalstu izlūkošanas iestādēm – it īpaši starp Lielbritānijas un Vācijas – un ASV iestādēm.[82]

Šie atklājumi iepriekš nebija zināmi ne tikai plašākai sabiedrībai, bet arī lielākajai daļai politisko lēmumu pieņēmēju un izraisīja globālu sašutumu. Vairāk nekā 1000 akadēmiskās sabiedrības pārstāvju parakstīja dokumentu, lai iebilstu pret masveida komunikāciju novērošanas praksi.[83] Arī starptautiskās organizācijas vērsa uzmanību uz šādas novērošanas prakses negatīvo ietekmi uz cilvēktiesībām. 2014. gadā ANO pieņēma ziņojumu, kurā nosoda nelikumīgu vai patvaļīgu komunikācijas uzraudzību un pārtveršanu, kā arī personas datu vākšanu, it īpaši, ja tā tiek veikta masveidā kā darbības, kas būtiski aizskar tiesības uz privātumu un vārda brīvību un var būt pretrunā ar demokrātiskas sabiedrības principiem.[84]

Līdz šim uzmanība pamatā ir pievērsta masveida novērošanai kā valsts un vēlāk arī privāto uzņēmumu piespiedu un pamatā slepenai varas īstenošanas formai. Tomēr līdz ar tās milzīgajiem apmēriem, kas turpina strauji augt, kā arī arvien plašāku akceptēšanu no sabiedrības puses, bet vienlaikus arī ar personu informētību mūsdienās tā ieņem citu formu un rada arī jaunus riskus personu tiesībām.

Modernās informācijas un komunikācijas tehnoloģijas tās atturošās ietekmes (*chilling effect* – angļu val.) dēļ var novest pie tā, ka indivīdi novēro un uzrauga cits citu un īsteno varu paši pār sevi bez jebkādas piespiešanas. Ne tikai tieša novērošana, bet arī apziņa, ka tevi var novērot, var likt personai mainīt savu uzvedību. Tas ir galvenais aspekts arī Džeremija Bentama (*Jeremy Bentham*) slavenajā *Panopticon* cietuma projektā, un tas arī bija attēlots Džordža Orvela (*George Orwell*) nozīmīgajā romānā "1984", kurā pilsoņi apzinājās, ka katru darbību var novērot policija, un tāpēc mēdza mainīt savu uzvedību.

Viens no ietekmīgākajiem uzraudzības pētniekiem ir Mišels Fuko (*Michel Foucault*), viņš veicināja pastiprinātu interesi par šo jomu. Fuko izmantoja Džeremija Bentama koncepciju par noteikta veida cietuma dizainu – panoptikonu –, kur sardzes tornis atrodas tieši apļveida cietuma centrā un kameras bez sienām ir vērstas uz iekšu. Uzraugi varēja vērot ieslodzītos, kuri nekad nezināja, vai viņi tiek novēroti. Ieslodzītie nevar zināt, vai kāds sēž centrālajā tornī un vai viņus vēro citi ieslodzītie no cietuma pagalma. Sociālā panoptikuma metafora ir tā,

82 Gellman, B., Poitras, L. (7 June, 2013). Washington Post: U.S., British intelligence mining data from nine US Internet companies in broad secret program. *Government Accountability Project.* https://whistleblower.org/in-the-news/washington-post-us-british-intelligence-mining-data-nine-us-internet-companies-broad/

83 Glaser, A. (12 February, 2014). Academics and Researchers Against Mass Surveillance. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2014/02/academics-and-researchers-against-mass-surveillance

84 OHCHR (2014), The right to privacy in the digital age.

ka novērošana neietver tikai zināmu vērotāju, kurš meklē, piemēram, aizdomās turēto, kurš pastāvīgi slēpjas, bet arī to, ka sabiedrība arvien vairāk tiek veidota tā, lai mudinātu mūs visus vērot citam citu.[85] Mūsdienu konteksts, ko raksturo arvien sarežģītāku novērošanas līdzekļu attīstība, vēl vairāk līdzinās Bentama "Panopticon" projektam nekā 19. un 20. gadsimta sabiedrība, kuru pētīja Fuko. Lielākā daļa novērošanas pētījumu akcentē Fuko panoptikona interpretācijas piespiedu vai represīvo pusi, kas uzsver varas būtisku pārsvaru. Tomēr viņš ir interpretējis to arī kā pašdisciplīnas praksi, kā to īpaši uzsver Bentams, tādējādi paplašinot "skatiena spēku", iekļaujot tajā visu veidu datu vākšanu un vizuālo novērošanu.[86]

No Bentama rakstiem par "panoptisko" vidi var secināt trīs galvenos elementus: "uzrauga" klātbūtne, ko nodrošina viņa pilnīga neredzamība; objektu universālā redzamība un pieņēmums, ka novērotie tiek novēroti pastāvīgi. Kaut arī varētu teikt, ka mums tagad ir daudz vairāk "novērotāju", ja ar redzamību mēs domājam iespēju piekļūt informācijai par personu – par viņa gaumi, interesēm, ienākumu līmeni, vecuma grupu, vēlamajām atpūtas aktivitātēm, vaļaspriekiem, politisko pārliecību, atrašanās vietu, iepirkšanās veidiem, interneta meklēšanas vēsturi, izmantotajām lietotnēm utt. Tas viss ir platformu kapitāla galvenais "izejmateriāls", kas tiek pastāvīgi vākts, apstrādāts un kas ir saistīts ar peļņu. Turklāt digitālās tehnoloģijas kā mūsdienu sabiedrības "panoptikas" iestatījumi nodrošina dažādus paškontroles un pašcenzūras veidus.[87]

Pašdisciplīnas un pašierobežošanas īstenošanai ir svarīgi, lai novērotie objekti saprastu, ka tie ir universāli un pastāvīgi redzami. Šāda apzināšanās ir notikusi, it īpaši pateicoties Edvardam Snoudenam, kurš atklāja NSA novērošanas apjomu, tostarp iegūstot datus no digitālajām platformām, piemēram, "Facebook", "Google", "Yahoo" utt., kā arī citiem prettiesiskiem "slēptiem" datu iegūšanas gadījumiem, piemēram, no politisko konsultāciju uzņēmuma "Cambridge Analytica" un "Facebook" skandāla. Šī apzināšanās rada "atturošu efektu" – lietotāju pašcenzūru – un īpaši ietekmē vārda brīvību. Jaunās tehnoloģijas arī mūsdienu sabiedrībā rada dažādus paškontroles un pašcenzūras veidus. Tādējādi mūsdienās būtiska atšķirība ir starp divām novērošanas formām – mērķtiecīgu konkrētu personu novērošanu un vispārīgāku jeb masveida novērošanu.

1.1.3.3. Mērķtiecīga un masveida novērošana

Tradicionālā jeb t. s. mērķtiecīga novērošana (*targeted surveillance* – angļu val.) ir nošķirama no masveida digitālās novērošanas (*mass surveillance* – angļu val.).

85 Moore, P. V. (2020). Data subjects, digital surveillance, AI and the future of work.

86 Manokha, I. (2018). Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance & Society*, 16(2), pp. 219–237. https://doi.org/10.24908/ss.v16i2.8346

87 Ibid.

Novērošana ir viena no galvenajām metodēm, ko izmanto tiesībaizsardzības iestādes, lai novērstu, izmeklētu un atklātu noziedzīgus nodarījumus.

Tradicionālā novērošanā tiek veikta aizdomās turēto personu vai iespējamo noziedzīgo darbību novērošana. Noziedzīgu nodarījumu atklāšanā sen jau tiek izmantoti personu attēli un videoieraksti. Videonovērošana, kas kļuva plaši pieejama 20. gadsimta 60. un 70. gados, ļāva tiesībaizsardzības iestādēm ātri identificēt personas un atklāt noziedzīgus nodarījumus.

Attīstoties tehnoloģijām, tiesībaizsardzības iestāžu darbība ir ļoti mainījusies. Ir izveidoti daudzi informācijas centri un sistēmas, kurās tiek vākti, apkopoti dati, kā arī notiek apmaiņa ar tiem, piemēram, no sodāmības reģistriem, biometriskajiem datiem, atrašanās vietas datiem, noziedzīgu nodarījumu novēršanas, izmeklēšanas un atklāšanas nolūkā. Tiek izmantotas tādas metodes kā slēpta sarunu noklausīšanās, telekomunikāciju un metadatu iegūšana.[88] Šāda novērošana tiek veikta visas sabiedrības interesēs, lai atklātu noziedzīgus nodarījumus un garantētu sabiedrisko drošību. Tā vienmēr sākas ar aizdomām pret konkrētu personu vai personām, un uz šo aizdomu pamata tiek veikta "mērķtiecīga" novērošana.

Mērķtiecīga novērošana var būt prettiesiska, patvaļīga un radīt negatīvas sekas personām. Kā ir atklāts vairākos ANO ziņojumos, ir pierādīts, ka personu (bieži vien žurnālistu, aktīvistu, opozīcijas pārstāvju, kritiķu un citu personu, kas izmanto savas tiesības uz vārda brīvību) novērošana noved pie patvaļīgas aizturēšanas, dažkārt pat spīdzināšanas un, iespējams, arī slepkavības bez tiesas.[89] Daudzās valstīs nav atbilstošu tiesību aktu vai arī tie netiek piemēroti, ir vājas procesuālās garantijas un neefektīva uzraudzība, un tas viss ir veicinājis atbildības trūkumu par nelikumīgu digitālo novērošanu. Šāda novērošana ir attīstījusies, vāji kontrolējot eksportu un tehnoloģiju nodošanu valdībām, kas īsteno plaši zināmas represijas politikas.

Turklāt šādu prettiesisku novērošanu netiešā veidā veicina un atbalsta ASV, kā arī citu demokrātisku valstu tehnoloģiju uzņēmumi, kas izstrādā un pārdod novērošanas tehnoloģijas valdībām, kuras tās savukārt izmantotu pret žurnālistiem, opozīcijas līderiem, aktīvistiem un citiem sabiedrības pārstāvjiem, kuriem ir nozīmīga loma demokrātiskā sabiedrībā. 2020. gada novembrī Eiropas Parlaments un Padome vienojās par jaunu tiesisko regulējumu, lai kontrolētu un ierobežotu tādu kibernovērošanas preču eksportu uz autoritāriem un represīviem režīmiem, kas ļauj "slēpti novērot fiziskas personas, novērojot, iegūstot, vācot vai

88 Sk., piemēram, UNODC. (2009). Current practices in electronic surveillance in the investigation of serious and organized crime. https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf

89 UN Human Rights Council. (2019). Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. https://digitallibrary.un.org/record/3814512#record-files-collapse-header

analizējot datus, tostarp biometriskos datus", un nepieļautu, ka šīs tehnoloģijas tiek izmantotas pretrunā ar cilvēktiesībām.[90]

Gan starptautiskā, gan nacionālā līmenī ir bijuši ilgstoši centieni regulēt valstu novērošanas pasākumus, ieviešot nepieciešamās aizsardzības garantijas, un izveidot regulējumu, lai nodrošinātu šādu pasākumu samērīgumu un atbilstību pamattiesībām. Demokrātiskās tiesiskās valstīs, lai veiktu mērķtiecīgu novērošanu noziedzīgu nodarījumu atklāšanas un izmeklēšanas interesēs, ir jāievēro stingri procesuālie noteikumi, to skaitā iepriekš jāsaņem tiesneša atļauja šādai novērošanai, lai nodrošinātu, ka personu tiesības netiek nesamērīgi ierobežotas vai pārkāptas. Tomēr, ja attiecībā uz tradicionālo novērošanu, kas tiek veikta noziedzīgu nodarījumu novēršanas un atklāšanas nolūkā, tas ir pamatā izdevies, tad daudz grūtāk ir vienoties par regulējumu un robežām masveida novērošanas pasākumiem, it īpaši tādiem, kas balstās uz mākslīgo intelekta sistēmu izmantošanu.

Masveida digitālā novērošana atšķiras no tradicionālās jeb mērķtiecīgās novērošanas. Tā ir sistemātiska cilvēku darbību un komunikācijas novērošana, kas īstenota, izmantojot informācijas un komunikācijas tehnoloģijas. Valstu veiktās masveida jeb stratēģiskās novērošanas galvenais mērķis ir proaktīvi identificēt "riskantas grupas", proti, tās mērķis ir identificēt iespējamas briesmas, nevis izmeklēt zināmus draudus. Masveida novērošanu var veikt arī tad, ja nepastāv aizdomas pret konkrētu personu vai personām.[91] Novērošana bieži vien ir saistīta ar personiskas informācijas iegūšanu un analīzi. Tā var ietvert dažādus personas dzīves aspektus, komunikāciju, informāciju par ceļošanu, finansiālo informāciju, darbībām internetā.

Eiropas Padome ir norādījusi, ka "pilsoņu masveida novērošana saskaņā ar ECTK ir pieļaujama tikai tad, ja tā ir absolūti jeb stingri nepieciešama demokrātisku institūciju aizsardzībai. Ņemot vērā, ka tā ievērojami apdraud ECTK nostiprinātās pamattiesības uz privātumu un vārda brīvību, dalībvalstīm ir jānodrošina, ka līdz ar novērošanas metožu attīstību, kā rezultātā notiek masveida datu

90 Stolton, S. (10 November 2020). EU to restrict sale of cyber-surveillance goods to repressive regimes. *EURACTIV.* https://www.euractiv.com/section/digital/news/eu-to-restrict-sale-of-cyber-surveillance-goods-to-repressive-regimes/; sk. arī Eiropas Parlamenta 2021. gada 25. marta normatīvo rezolūciju par priekšlikumu Eiropas Parlamenta un Padomes regulai, ar ko izveido Savienības režīmu divējāda lietojuma preču eksporta, pārvadājumu, starpniecības, tehniskās palīdzības un tranzīta kontrolei (pārstrādāta redakcija). https://www.europarl.europa.eu/doceo/document/TA-9-2021-0101_LV.html

91 Council of Europe. (2018). Mass Surveillance. https://rm.coe.int/factsheet-on-mass-surveillance-june2018-docx/16808b3dd8

vākšana, vienlaikus tiek izstrādāti arī tiesiski aizsardzības pasākumi, kas nodrošina cilvēka cieņas ievērošanu."[92]

Vai valstīm ir nepieciešams veikt masveida novērošanu, lai iedzīvotāji varētu būt drošībā? Par šo jautājumu ir ilgstoši diskutējuši cilvēktiesību aizstāvji, kā arī starptautiskās organizācijas un tiesas. Vēl vairāk šis jautājums ir kļuvis aktuāls līdz ar jauno tehnoloģiju, it īpaši sejas atpazīšanas un citu biometrisko tehnoloģiju, izmantošanu masveida novērošanai, ņemot vērā, ka tās rada vēl ievērojamāku apdraudējumu cilvēktiesībām.

AI HLEG vērš uzmanību, ka uzticama mākslīgā intelekta sasniegšanai ir svarīgi skaidri definēt, vai, kad un kā mākslīgo intelektu var izmantot, lai automātiski identificētu cilvēkus, un nošķirt personas identificēšu no tās izsekošanas, kā arī mērķtiecīgu novērošanu no masveida novērošanas.[93]

Eiropas Parlamenta piedāvātajā Priekšlikumā Eiropas Parlamenta un Padomes Regulai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrādes, ieviešanas un izmantošanas ētikas principiem tika norādīts, ka biometrisko datu izmantošana un vākšana attālinātās identifikācijas nolūkos publiskās vietās, izmantojot biometrisko vai sejas atpazīšanu, īpaši apdraud pamattiesības un ka dalībvalstu publiskās iestādes tās var ieviest vai izmantot, tikai ja tas ir nepieciešams, lai sasniegtu būtiskas sabiedrības intereses.[94]

Mākslīgā intelekta sistēmu izmantošana rada būtisku apdraudējumu, kas pamato nepieciešamību tās stingrāk regulēt un pat konkrētos gadījumos aizliegt to izmantošanu, lai nepieļautu, ka valsts iestādes tās mēģina ieviest, nepamatoti atsaucoties uz būtisku sabiedrības interešu aizsardzību. Šie jautājumi sīkāk apskatīti grāmatas turpmākajās nodaļās. Savukārt šīs nodaļas turpinājumā atklāts, kā valstis bieži vien nepamatoti kā argumentu izmanto nacionālās un sabiedrības drošības intereses, lai ieviestu masveida novērošanas pasākumus.

1.1.3.4. Drošība kā pamats valsts novērošanai

Masveida novērošanas pasākumus valstis ir ieviesušas pamatā ar mērķi novērst arvien pieaugošos draudus valsts un sabiedrības drošībai, it sevišķi, lai cīnītos pret terorismu. Pēc 2001. gada 11. septembra teroristu uzbrukumiem ASV sāka izmantot savu varu, lai veiktu masveida elektronisko novērošanu un sakaru pārtveršanu gan no ASV, gan citām pasaules valstīm. ASV masveida novērošanas prakse ir pamatā diviem EST nolēmumiem, kas tika pieņemti 2015. gadā "Schrems I" lietā un 2020. gadā "Schrems II" lietā. Ar šiem nolēmumiem par spēkā neesošiem

92 Council of Europe. (2018). Mass Surveillance. https://rm.coe.int/factsheet-on-mass-surveillance-june2018-docx/16808b3dd8

93 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

94 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

divas reizes tika atzīti Eiropas Komisijas lēmumi par aizsardzības līmeņa pietiekamību datu nodošanai uz ASV, kas veidoja pamatu datu nodošanai no ES uz ASV. Eksteritoriālās digitālās masveida novērošanas atklāšana ir sagrāvusi uzticību transatlantiskajām attiecībām un radījusi jautājumus arī par citu ilgtermiņa līgumu, kas paredz datu nodošanu starp ASV un ES, likumību, tostarp par Teroristu finansēšanas izsekošanas programmas nolīguma[95] un Pasažieru datu reģistra nolīguma[96] īstenošanu.

ES arī ir ieviesusi masveida novērošanas pasākumus drošības interešu vārdā. Nepieciešamība cīnīties pret terorismu ir novedusi pie datu saglabāšanas shēmu ieviešanas, kas paredz apmaiņu ar izlūkdienestu informāciju, masveida datu vākšanu un liela mēroga datubāzu izveidi ES, un tas viss veido nozīmīgu daļu no ES pretterorisma politikas. Nepieciešamība apkarot terorismu bija pamatā ES datu saglabāšanas režīmu ieviešanai, kas ļāva dalībvalstīm uzraudzīt elektroniskos sakarus drošības nolūkos. Kā steidzamu pretterorisma pasākumu, reaģējot uz teroristu uzbrukumiem 2004. gadā Madridē un 2005. gadā Londonā, ES pieņēma Datu saglabāšanas direktīvu[97]. Lai gan bija izteiktas bažas, ka šāda masveida novērošanas pasākuma ieviešana neatbilst pamattiesībām, tomēr, ņemot vērā milzīgo politisko spiedienu, direktīva tika ātri pieņemta un stājās spēkā 2006. gadā. Datu saglabāšanas direktīva pieprasīja dalībvalstīm uzlikt telekomunikāciju un interneta pakalpojumu sniedzējiem pienākumu saglabāt konkrētu kategoriju datus par mobilo un fiksēto telefonu sarunām un lietotāju atrašanās vietu, piekļuvi internetam un e-pasta lietošanu, kas neietver komunikācijas saturu, bet metadatus saglabāt vismaz sešus mēnešus un ne ilgāk kā divus gadus, un pēc pieprasījuma tos darīt pieejamus tiesībaizsardzības iestādēm smagu noziegumu un terorisma izmeklēšanas, atklāšanas un kriminālvajāšanas nolūkos. 2014. gadā EST pieņēma sprieduma apvienotajās lietās "Digital Rights Ireland" un "Seitlinger u. c.", ar kuru pasludināja Datu saglabāšanas direktīvu par spēkā neesošu, atzīstot, ka tā rada nepamatotu iejaukšanos pamattiesībās.[98]

95 Nolīgums starp Eiropas Savienību un Amerikas Savienotajām Valstīm par tādu finanšu ziņojumapmaiņas datu apstrādi un nodošanu, kurus Eiropas Savienība dara pieejamus Amerikas Savienotajām Valstīm, lai īstenotu Teroristu finansēšanas izsekošanas programmu. OV L 8, 13.01.2010. (spēkā līdz 31.10.2010.).

96 Nolīgums starp Amerikas Savienotajām Valstīm un Eiropas Savienību par pasažieru datu reģistra datu izmantošanu un pārsūtīšanu Amerikas Savienoto Valstu Iekšzemes drošības departamentam. *OV L* 215, 11.8.2012.

97 Eiropas Parlamenta un Padomes Direktīva 2006/24/EK (2006. gada 15. marts) par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK. *OV L* 105, 13.04.2006. (spēkā līdz 03.05.2006.).

98 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C293/12 .. Eiropas Savienības Tiesas prakse atsevišķi analizēta darba piektajā nodaļā.

EST ir izskatījusi daudzas lietas par elektronisko datu saglabāšanas režīmiem. 2020. gada oktobrī EST pieņēma nolēmumus, kuros izvērtēja Apvienotās Karalistes, Francijas un Beļģijas "liela apjoma" jeb masveida datu vākšanas vai saglabāšanas režīmu valsts drošības kontekstā atbilstību privātuma garantijām saskaņā ar ES tiesībām.[99] EST ir atzinusi, ka policijai un izlūkošanas iestādēm ir ļoti svarīga loma mūsu drošības garantēšanai, tomēr tām ir jādarbojas saskaņā ar noteiktām garantijām, lai novērstu to ļoti ievērojamās varas ļaunprātīgu izmantošanu. Tām būtu jākoncentrējas uz efektīvu un mērķtiecīgu novērošanas sistēmu nodrošināšanu, kas aizsargā gan mūsu drošību, gan pamattiesības. Demokrātiskā sabiedrībā neviena valsts varas iestāde nevar būt augstāka par likumu un ir jānosaka ierobežojumi un kontrole policijas un izlūkošanas iestāžu novērošanas pilnvarām.

Latvijas tiesību zinātnieks un bijušais Latvijas Republikas Satversmes tiesas tiesnesis asociētais profesors Uldis Ķinis uzsver, ka "demokrātiskā un tiesiskā valstī drošība iespējama tikai tad, ja sabiedrībā tiek garantētas cilvēktiesības un ievēroti vispārīgie tiesību principi".[100]

Līdzās regulējumam, kas saistīts ar elektroniskās komunikācijas saglabāšanas režīmiem, kritiku ir izraisījuši arī citi ES tiesību akti, kas paredz masveida datu saglabāšanu. Ļoti pretrunīgi vērtēta ir ES pasažieru datu reģistra sistēma, kas bija ES politikas reakcija uz traģiskajiem teroristu uzbrukumiem visā pasaulē un Eiropā, īpaši Parīzē un Briselē, kā arī pasažieru datu nolīgumi ar trešajām valstīm, tostarp ASV un Austrāliju. 2017. gadā EST secināja, ka ES un Kanādas Pasažieru datu reģistra nolīgums neatbilst Eiropas Savienības Pamattiesību hartas (Harta) 7. un 8. pantā noteiktajām tiesībām uz privātumu un datu aizsardzību. Ir kritizēti arī priekšlikumi regulai par personas apliecību un citu dokumentu drošības uzlabošanu, kas paredz biometrisko datu apstrādi[101], regulai, ar ko groza vīzu informācijas sistēmu[102], u. c. Tomēr ES līmenī pieņemtie pasākumi tiek daudz rūpīgāk izvērtēti un uzraudzīti nekā pasākumi, ko pieņem valstis nacionālā līmenī, īpaši saistībā ar lielo datu un jauno tehnoloģiju sniegtajām iespējām.

99 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C511/18 *La Quadrature du Net* u. c., C-512/18 *French Data Network* u. c. un C-520/18 *Ordre des barreaux francophones et germanophone* u. c., ECLI:EU:C:2020:791.

100 Ķinis, U. Kiberdrošība – tiesiski aizsargājama vērtība. *Jurista Vārds.* 06.10.2020., Nr. 40.

101 Eiropas Datu aizsardzības uzraudzītājs. (2018). Eiropas Datu aizsardzības uzraudzītāja atzinuma kopsavilkums par priekšlikumu regulai par Savienības pilsoņu personas apliecību un citu dokumentu drošības uzlabošanu. https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_summary_lv_0.pdf

102 FRA. (2018). The revised Visa Information System and its fundamental rights implications. https://fra.europa.eu/en/opinion/2018/visa-system

Dažādus uzraudzības pasākumus drošības interesēs plaši ievieš gan ES, gan atsevišķas valstis. Sākoties Covid-19 pandēmijai 2020. gadā, mēs varējām sekot līdzi neskaitāmiem piemēriem, kad valstis ieviesa jaunus masveida novērošanas pasākumus. Tie aplūkoti atsevišķi nodaļas turpinājumā.

Teroristu uzbrukumu draudi ir bieži izmantots arguments, lai pamatotu jaunu novērošanas pasākumu, tostarp mākslīgā intelekta novērošanas tehnoloģiju, izmantošanu. Piemēram, tūlīt pēc asiņainajiem uzbrukumiem Francijas pilsētā Nicā 2020. gada oktobrī, kuru laikā ar nazi tika nogalināti vairāki cilvēki, politiķi, to skaitā prezidenta Emanuela Makrona (*Emmanuel Macron*) valdības ministrs, aicināja izmantot mākslīgā intelekta sejas atpazīšanas tehnoloģijas, piemēram, sabiedriskajā transportā, lai veiktu iespējamo uzbrucēju novērošanu un novērstu turpmāku vardarbību un terorismu. Pirms gada, 2019. gada oktobrī, Nicā jau tika veikti eksperimenti, izvietojot sejas atpazīšanas kameras pie vidusskolas ieejas, bet tie tika pārtraukti pēc Francijas datu aizsardzības iestādes CNIL (*Commission Nationale de l'Informatique et des Libertés*) iejaukšanās. Sejas atpazīšanas tehnoloģiju izvietošana sabiedriskās vietās tika atzīta par nevajadzīgu un nesamērīgu, lai sasniegtu to noteikto mērķi – drošību. Pēc uzbrukumiem šis uzraudzības iestādes viedoklis tika kritizēts.

Nacionālās un sabiedrības drošības garantēšana vienmēr ir bijis neapstrīdams arguments, lai iedzīvotājus, kas dzīvo bailēs par savu drošību, varētu pārliecināt, ka novērošanas tehnoloģijas ir nepieciešamas viņu aizsardzībai. Līdzšinējā prakse rāda, ka masveida komunikācijas novērošanas pasākumi, kas tika ieviesti ar mērķi aizsargāt valsts un sabiedrības drošību, ir izrādījušies neefektīvi terorisma apkarošanai.[103] Tomēr, ja uz spēles tiek likta drošība, citi argumenti, piemēram, personu pamattiesību aizsardzība, vienmēr liksies mazāk svarīgi.

Saskaroties ar drošības apdraudējumu, valstīm vienmēr ir bijusi vēlēšanās strauji ieviest jaunus uzraudzības pasākumus, bet vēl vairāk šo tendenci ir ietekmējušas jauno tehnoloģiju radītās iespējas. Turpinājumā atklāts, kādā veidā jaunās tehnoloģijas ir ievērojami palielinājušas novērošanas praksi, radot jaunus būtiskus izaicinājumus, kam ir jāmeklē risinājumi.

103 Vinocur, N. (30 October, 2020). French politicians urge deployment of surveillance technology after series of attacks. *POLITICO.* https://www.politico.eu/article/french-politicians-urge-deployment-of-surveillance-technology-after-series-of-attacks/

1.2. Mākslīgā intelekta novērošanas tehnoloģijas

1.2.1. Mākslīgais intelekts kā "degviela" valsts novērošanai

Mākslīgā intelekta tehnoloģiju straujā attīstība ievērojami veicina jaunu novērošanas pasākumu ieviešanu un izmantošanu. Tās ļauj masveida novērošanu veikt ievērojami plašāk, detalizētāk un precīzāk analizēt dažādas īpašības un pazīmes daudzās jomās un dažkārt arī iepriekš nenojaustiem mērķiem. Šādu novērošanu var saukt par "gudro uzraudzību" (*smart surveillance* – angļu val.), uzsverot, ka šie jaunie risinājumi ir "inteliģenti" tādā nozīmē, ka tie, šķiet, mācās no novērotajiem datiem, kā arī paši "pieņem lēmumus", balstoties uz noteiktiem algoritmiem.

Mākslīgais intelekts uzlabo tiesībaizsardzības, drošības un izlūkošanas iestāžu novērošanas iespējas. Šīs iestādes sistemātiski ir izmantojušas datu analīzi, lai veiktu prognozēšanu, profilēšanu un preventīvu novērošanu. Mašīnu mācīšanās un dziļās mācīšanās algoritmi ievērojami veicina novērošanas iespējas. Tie rada jaunas tehnoloģiskās iespējas lielo datu kopu izveidei, apstrādei un izmantošanai unikālos un neizpētītos veidos, lai veiktu izvērtēšanu un prognozes par cilvēkiem, bieži vien bez pierādījumiem par to saistību ar noziedzību. Turklāt mākslīgā intelektā balstītas tehnoloģijas nebūt nav nekļūdīgas.

Arvien vairāk valstu novērošanas vajadzībām izmanto mākslīgā intelekta tehnoloģijas – sejas atpazīšanas sistēmas, viedās pilsētas platformas, viedo policiju, automatizētās robežkontroles sistēmas. Kārnegija Starptautiskā miera fonda (*Carnegie's Endowment for International Peace*) pētnieka Stīvena Feldšteina (*Steven Feldstein*) 2019. gada septembrī publicētais pētījums parādīja, ka vismaz 75 no 176 pasaules valstīm aktīvi izmanto mākslīgā intelekta tehnoloģijas novērošanas vajadzībām. Pētījums atklāj, ka 56 valstis ir ieviesušas viedās pilsētas jeb drošas pilsētas platformas, 64 valstis – sejas atpazīšanas sistēmas un 52 valstis – viedo tiesībaizsardzību (*smart policing* – angļu val.).[104] Šis skaits strauji palielinās, jo arvien vairāk valstu ievieš mākslīgā intelekta novērošanas tehnoloģijas.

It sevišķi valstis ar autoritārām sistēmām un zemu politisko tiesību līmeni iegulda daudz līdzekļu mākslīgā intelekta novērošanas sistēmās. Ķīna ir galvenais mākslīgā intelekta novērošanas virzītājspēks visā pasaulē. Modernas analītiskās sistēmas, sejas atpazīšanas kameras un sarežģītas novērošanas sistēmas iegādājušās daudzas Persijas līča, Austrumāzijas, Dienvidāzijas un Centrālāzijas valdības. Bet arī liberālās demokrātiskās Eiropas valstis arvien plašāk ievieš sejas atpazīšanas sistēmas, automatizētas robežkontroles sistēmas, prognozēšanas sistēmas tiesībaizsardzības nolūkos un drošas pilsētas sistēmas.

Mākslīgā intelekta novērošanas tehnoloģijas, kas vāc un apstrādā biometriskos datus, rada jauna veida būtisku apdraudējumu cilvēktiesībām. Pēdējie gadi

104 Feldstein (2019), The Global Expansion of AI surveillance.

iezīmē pagrieziena punktu, kad varam novērot arvien plašāku biometrisko datu izmantošanu, un šī tendence turpina tikai palielināties. Turpmāk arvien straujāk pieaugs mākslīgā intelekta sistēmu izstrādes, ieviešanas un izmantošanas rezultātā iegūtu biometrisko datu ģenerēšana un izmantošana.

Visplašākās diskusijas un kritika visā pasaulē ir par sejas atpazīšanas tehnoloģijām, kas vāc un izmanto biometriskos datus attālinātās identifikācijas nolūkos sabiedriskās vietās. Dažkārt tiesībaizsardzības iestādes un policija sejas atpazīšanas tehnoloģijas izmanto arī kā prognozēšanas rīku, kas analizē un izvērtē iedzīvotāju uzvedību. Šo novērošanas tehnoloģiju izmantošana aplūkota nodaļas turpinājumā.

1.2.2. Sejas atpazīšanas tehnoloģijas

Cilvēku spēja paust emocijas, tostarp ar sejas izteiksmes palīdzību, ir ļāvusi mums kā sabiedriskām būtnēm savā starpā komunicēt. Gadsimtiem tā ir bijusi arī iedvesmas avots neskaitāmiem izciliem mākslas darbiem. Atliek vien atcerēties slepeno smaidu Leonardo da Vinči (*Leonardo da Vinci*) slavenajā gleznā "Mona Liza". Tomēr mūsdienās mākslīgā intelekta pasaulē ir parādījušies jauni, daudz mazāk iedvesmojoši un emocionāli tās izmantošanas veidi. Cilvēka seja ir kļuvusi par datu avotu, ko izmanto gan valsts iestādes, gan privātie uzņēmumi, izstrādājot un ieviešot jaunas tehnoloģijas, veidojot novērošanas sabiedrību.

Mūsu sejas attēls, ar kuru mēs vienmēr esam varējuši brīvi rīkoties un kas ļauj mums sazināties, paust emocijas un iekšējās izjūtas dažādās situācijās, vai tās būtu prieks, sajūsma, pārsteigums, aizrautība, pateicība vai arī vienaldzība, neizpratne, bēdas, nožēla, dusmas, vienmēr ir piederējis tikai mums pašiem. Tomēr tagad arvien nenovēršamāk tas tiek izmantots, lai izstrādātu un ieviestu mākslīgā intelekta tehnoloģijas, veidotu datubāzes un trenētu algoritmus.

Sejas atpazīšana ir biometriska tehnoloģija, kas izmanto algoritmus un mašīnmācīšanos, lai identificētu personas no fotoattēla vai video. Tā ļauj salīdzināt digitālos sejas attēlus, lai noskaidrotu, vai tā ir viena un tā pati persona. Sejas atpazīšanas tehnoloģija ļauj, piemēram, tiesībaizsardzības iestādēm identificēt personas, salīdzinot viņu attēlus, kas uzņemti ar videonovērošanas kamerām, kuras uzstādītas sabiedriskās vietās, ar biometriskiem attēliem, kuri glabājas informācijas tehnoloģiju sistēmās.

Sejas atpazīšanas sistēmas izmanto skaitļošanas algoritmus, parasti mašīnmācīšanās modeļus, lai atlasītu unikālas personas sejas identifikācijas detaļas. Sejas atpazīšanas procesā ir vairāki soļi ar trim pamatdarbībām: sejas noteikšanu, sejas fiksēšanu un sejas salīdzināšanu. Pirmais solis ir sejas attēla uzņemšana, to nofotografējot vai nofilmējot. Attīstītas tehnoloģijas ļauj atpazīt sejas pūlī vai pat pēc kāda silueta. Otrais solis ir sejas ģeometrijas nolasīšana, izmantojot

sejas atpazīšanas programmatūru. Galvenie faktori ietver attālumu starp acīm un attālumu no pieres līdz zodam. Rezultāts ir "individuāls paraksts". Šis paraksts, kas faktiski ir matemātiska formula, pēc tam tiek salīdzināts ar zināmiem sejas attēliem datubāzē. Pamatojoties uz uzņemtā modeļa un atrasto datu līdzību, var noteikt atbilstību starp novērošanas kameras uzņemto attēlu un konkrēto sejas attēlu datubāzē. Neatkarīgi no paredzētā mērķa apstrādes darbības, ko veic šāda veida tehnoloģija, ir gandrīz vienādas.[105]

Sejas atpazīšanas tehnoloģijas arvien plašāk ievieš un izmanto dažādiem mērķiem gan valsts iestādes, gan privātie uzņēmumi. Sejas atpazīšana kā biometriskās autentifikācijas tehnoloģija ir izmantota jaunākajos viedtālruņos, ļaujot to lietotājiem atbloķēt savas ierīces, un dažas bankas to izmanto darījumu autorizēšanai. ASV, kā arī Eiropas lidostās tiek ieviestas un testētas sejas atpazīšanas sistēmas pasažieru identitātes pārbaudei, lai paātrinātu iekāpšanu, kā arī tās tiek izmantotas, lai piedāvātu pasažieriem personalizētus pakalpojumus.[106] Ne tikai privātie uzņēmumi, bet arī valstis ir sākušas izmantot sejas atpazīšanas tehnoloģiju identitātes pārbaudei. 2020. gada rudenī Singapūra paziņoja, ka būs pirmā valsts, kas sejas atpazīšanu izmantos personu identitātes pārbaudei.[107]

Sejas atpazīšanas sistēmas ir ieviesuši arī daudzi lielie sociālo mediju uzņēmumi, izraisot skaļus protestus. "Facebook" ieviesa sejas atpazīšanu, kas nosaka cilvēku vārdus augšupielādētās fotogrāfijās. ASV Ilinoisas štata iedzīvotāji iesniedza prasību tiesā pret "Facebook" par biometrisko datu apstrādi bez viņu piekrišanas. Lai izbeigtu tiesvedību, pamatojoties uz vienošanos, "Facebook" piedāvāja

105 Sejas atpazīšanas sistēma veic šādas datu apstrādes darbības:
a) attēlu iegūšana: indivīda sejas attēla uzņemšana un pārveidošana par digitālu attēlu;
b) sejas attēla noteikšana: sejas attēla noteikšana digitālajā attēlā un zonas marķēšana;
c) normalizēšana: lai izlīdzinātu noteikto sejas reģionu variācijas, piemēram, attēla pārveidošana standarta izmērā vai pat krāsu sadalījumu pagriešana vai izlīdzināšana;
d) atribūtu iegūšana (pazīmes): lai izolētu un izveidotu atkārtojamus rādījumus, kas atšķiras no indivīda digitālā attēla. Atribūtu kopa ir definēta kā veidne salīdzinājumiem ar sejas datubāzi – sejas parakstu;
e) glabāšana: ja indivīda seja tiek uzņemta pirmo reizi, attēlu un/vai atsauces modeli var saglabāt kā ierakstu turpmākiem salīdzinājumiem;
f) salīdzinājums: līdzības noteikšana starp paraugu un citu sistēmā iepriekš iekļautu modeli. Šo salīdzinājumu var veikt: 1) identifikācijai, 2) autentifikācijai vai pārbaudei un/vai 3) kategorizācijai.
Moraes, T. G., Almeida, E. C., de Pereira, J. R. L. (2021). Smile, You Are Being Identified! Risks and Measures for the Use of Facial Recognition in (Semi-)Public Spaces. *AI and Ethics, 1*, pp. 159–172. https://doi.org/10.1007/s43681-020-00014-3

106 Sk., piemēram, CNIL. (9 Octobre, 2020). Reconnaissance faciale dans les aéroports : quels enjeux et quels grands principes à respecter ? https://www.cnil.fr/fr/reconnaissance-faciale-dans-les-aeroports-quels-enjeux-et-quels-grands-principes-respecter

107 McDonald, T. (25 September, 2020). Singapore in world first for facial verification. *BBC News.* https://www.bbc.com/news/business-54266602

samaksāt 650 miljonus ASV dolāru.[108] Līdzīga prasība par biometrisko datu pretiesisku izmantošanu tika ierosināta arī pret "Instagram".[109] Tiesvedības ir ierosinātas arī pret tādiem tehnoloģiju milžiem kā "Microsoft", "Google" un "Amazon" par cilvēku attēlu izmantošanu bez piekrišanas, lai apmācītu tehnoloģijas.[110] Šīs tehnoloģijas tiek ieviestas arī iepirkšanās centros, lielveikalos, bibliotēkās un pat skolās, radot arī plašus protestus un pirmos datu uzraudzības iestāžu lēmumus, kas aizliedz to izmantošanu.[111]

Sejas atpazīšanas tehnoloģijas arvien plašāk izmanto arī policijas un citas tiesībaizsardzības iestādes ar mērķi garantēt sabiedrības drošību un cīnīties pret terorismu. Jau pieminētā Kārnegija Starptautiskā miera fonda pētnieka Stīvena Feldšteina 2019. gada septembrī publicētā aptauja liecina, ka vismaz 64 pasaules valstis novērošanas vajadzībām izmanto sejas atpazīšanas tehnoloģijas.[112] Tās tiek ieviestas visā pasaulē – ASV, Japānā, Singapūrā, Apvienotajos Arābu Emirātos, Krievijā, Ķīnā, kur mākslīgā intelekta novērošanas tehnoloģijas attīstītās visstraujāk, un daudzās citās valstīs. Simtiem pilsētu, lai cīnītos ar noziedzību, ir uzstādījušas kameras, kas aprīkotas ar sejas atpazīšanas tehnoloģijām, solot sniegt datus centrālajiem vadības centriem kā "drošas pilsētas" vai "gudras pilsētas" risinājumu. Visprogresīvākā šī tendence ir Ķīnā, kur 2019. gadā vairāk nekā 100 pilsētas iegādājās sejas atpazīšanas novērošanas sistēmas. Arī daudzas Eiropas valstis izstrādā un testē šīs tehnoloģijas sabiedriskās vietās drošības nolūkos, piemēram, Francija, Vācija, Spānija, Nīderlande un it īpaši Lielbritānija, un šo valstu skaits aizvien pieaug. Sabiedriskās organizācijas "AlgorithmWatch" 2019. gada pētījums liecina, ka no 27 ES dalībvalstīm vismaz 11 valstīs policijas iestādes izmanto sejas atpazīšanas tehnoloģijas, bet vēl astoņas plāno to ieviest nākamajos gados.[113] Šis skaits turpina pieaugt.

108 Moyer, E. (27 February, 2021). Facebook privacy lawsuit over facial recognition leads to $650M settlement. *Reuters.* https://www.reuters.com/article/us-facebook-privacy-lawsuit-idUSKCN25G08M

109 Holmes, A. (12 August, 2020). Instagram could face up to $500 billion in fines in class-action lawsuit alleging it illegally harvested biometric data. *Insider.* https://www.businessinsider.com/instagram-facing-500-billion-in-fines-in-facial-recognition-lawsuit-2020-8

110 Musil, S. (14 July, 2020). Amazon, Google, Microsoft sued over photos in facial recognition database. *CNET*. https://www.cnet.com/news/amazon-google-and-microsoft-sued-over-photos-in-facial-recognition-database/

111 EDPB (22 August, 2019), Facial recognition in school renders Sweden's ..; CNIL. (29 Octobre, 2019). Expérimentation de la reconnaissance faciale ..

112 Feldstein (2019), The Global Expansion of AI surveillance.

113 Kayser-Bril, N. (18 June, 2020). At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals. *Algorithm Watch.* https://algorithmwatch.org/en/face-recognition-police-europe/

Saraksti, kurus policija izmanto attēlu pārbaudei, var būt ļoti apjomīgi, un tajos var būt iekļauti cilvēki bez viņu ziņas. Džordžtaunas Universitātes Privātuma un tehnoloģiju centra Vašingtonā (*Center on Privacy and Technology at Georgetown University in Washington DC*) pētnieki 2016. gadā aprēķinājuši, ka aptuveni puse visu amerikāņu varētu atrasties tiesībaizsardzības iestāžu sejas atpazīšanas tīklos, jo daudzi štati ļauj policijai veikt meklēšanu autovadītāju apliecību datubāzēs.

2020. gada sākumā "The New York Times" atklāja, ka programmatūras uzņēmums "Clearview AI" Ņujorkā ir ieguvis miljardiem attēlu no sociālo mediju vietnēm un apkopojis tos sejas atpazīšanas datubāzē. Uzņēmums piedāvāja savus pakalpojumus policijai gan ASV, gan citām valstīm. Sociālo mediju platformas, piemēram, "Twitter", "Facebook" un "YouTube", pieprasīja "Clearview AI" pārtraukt iegūt attēlus no to vietnēm, norādot, ka tas pārkāpj viņu pakalpojumu sniegšanas noteikumus. Cilvēktiesību aizsardzības organizācijas pret uzņēmumu ir ierosinājušas vairākas tiesas prāvas gan Eiropā, gan ASV. Šāda tiesvedība tika ierosināta, piemēram, par Ilinoisas iedzīvotāju biometriskās informācijas – sejas attēlu – izmantošanu bez piekrišanas.[114]

2020. gada jūnijā arī Eiropas Datu aizsardzības kolēģija (*European Data Protection Board*) nāca klajā ar atzinumu, ka "Clearview AI" pakalpojums pārkāpj VDAR noteikumus.[115] "Clearview AI" paziņoja, ka ir pārtraucis šī pakalpojuma sniegšanu un attēlu meklētājprogramma darbojas likumu robežās. Zviedrijas datu uzraudzības iestāde 2021. gada februārī konstatēja, ka Zviedrijas Policijas pārvalde ir pārkāpusi datu aizsardzības noteikumus, izmantojot "Clearview AI" personu identificēšanai.[116]

"Clearview AI" nav vienīgais uzņēmums, kas ir ieguvis cilvēku seju attēlus šādā veidā. Polijas uzņēmumam "PimEyes" ir vietne, kas ikvienam ļauj atrast fotogrāfijas, un uzņēmums apgalvo, ka tā ir ieguvusi 900 miljonus attēlu, kaut arī, kā tā apgalvo, ne no sociālo mediju vietnēm. Savukārt "NtechLab" 2016. gadā izveidoja lietotni "FindFace", lai atļautu veikt sejas salīdzināšanu Krievijas sociālajā tīklā "VKontakte", kuras darbību vēlāk uzņēmums pārtrauca.[117]

114 Statt, N. (28 May 2020). ACLU sues facial recognition firm Clearview AI, calling it a 'nightmare scenario' for privacy. *The Verge.* https://www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws

115 EDPB. (10 June, 2020). Response to MEPs Sophie in 't Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI. https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en

116 EDPB (21 February, 2021), Swedish DPA ..

117 Roussi, A. (18 November, 2020). Resisting the rise of facial recognition. *Nature.* https://www.nature.com/articles/d41586-020-03188-2

Sejas atpazīšana galvenokārt tiek izmantota kriminālizmeklēšanā. Francijas pilsētā Lionā ar tās palīdzību tiek izmeklētas automašīnu zādzības. Īrijā to parasti izmanto, lai atklātu krāpniekus, kas pieprasa sociālos pabalstus, lietojot vairākas identitātes.[118] Pēdējos gados arvien izplatītāka kļūst automatizēta sejas atpazīšana reāllaikā (*live facial recognition* – angļu val.). Šo tehnoloģiju izmanto ne tikai pilsētu ielās, bet arī mūzikas koncertos, piemēram, Eda Šīrana (*Ed Sheeran*) koncertā, kā arī sporta sacensību laikā.[119] Gan ASV, gan Eiropā, piemēram, Itālijā, Vācijā, to izmanto pie futbola stadioniem, lai atrastu cilvēkus, kuri ir iekļauti vardarbīgu sporta līdzjutēju sarakstos.

Īpaši plaši reāllaika sejas atpazīšana tiek izmantota Apvienotajā Karalistē, kur ir ilga pieredze modernu novērošanas tehnoloģiju izmēģināšanā. Londonā pirmo reizi videonovērošanas sistēmas (CCTV) kameras policija uzstādīja 1953. gadā karalienes kronēšanas laikā un sāka pastāvīgi uzstādīt pagājušā gadsimta 60. gados. Londonā vēl nesen bija visvairāk novērošanas kameru uz vienu iedzīvotāju, ja salīdzina ar citām pasaules valstīm. Metropolitēna policijas dienests pirmo reizi izmantoja tehnoloģiju Notinghilas karnevālā 2016. gada augustā, un Dienvidvelsas policija pirmo reizi to izvietoja UEFA Čempionu līgas finālā 2017. gada jūnijā. Metropolitēna policijas dienests no 2016. gada līdz 2019. gadam veica desmit reāllaika sejas atpazīšanas testu sērijas, pārejot uz operatīvo izvietošanu 2020. gada sākumā. Dienvidvelsas policija to arī izmanto kopš 2017. gada galvenokārt lielos koncertos, festivālos un sporta pasākumos.[120] Abas policijas iestādes izmanto sejas atpazīšanu reāllaikā, konkrētā ierobežotā teritorijā un ierobežotu laika posmu, parasti izvietojot furgonu ar CCTV kamerām, izmantojot programmatūru, kas ļauj sejas attēlus no novērošanas saraksta salīdzināt ar seju attēliem, kas reāllaikā iegūti no CCTV plūsmas. Sejas atpazīšanas sistēma nav integrēta esošajās novērošanas sistēmās, piemēram, videonovērošanā.

2018. gadā Apvienotās Karalistes datu aizsardzības iestāde – Informācijas komisāra birojs (*Information Commissioner's Office*, ICO) – uzsāka izmeklēšanu pret abām policijas iestādēm par sejas atpazīšanas izmantošanu. 2020. gadā ICO publicēja ziņojumu, kurā vērsa uzmanību, ka policijas spēkiem ir "jāpiebremzē" un jāpamato šīs tehnoloģijas izmantošana. Tajā pašā laikā iestāde neaizliedza

118 Deegan, G. (11 September, 2018). Facial imaging software detects 28 cases of welfare fraud in 2018. *The Irish Times.* https://www.irishtimes.com/news/crime-and-law/facial-imaging-software-detects-28-cases-of-welfare-fraud-in-2018-1.3626076

119 Burgess, M. (4 September, 2019). UK police can use controversial facial recognition tech, court rules. *WIRED.* https://www.wired.co.uk/article/police-facial-recognition-south-wales-court-decision

120 Fussey, P., Murray, D. (2020). Policing Uses of Live Facial Recognition in the United Kingdom. In: Kak, A. (ed.), *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute, pp. 78–85. https://ainowinstitute.org/regulatingbiometrics.html

policijai izmantot šo tehnoloģiju, tikai norādīja uz prasībām, kuras nepieciešams ievērot. Tajā pašā laikā ICO arī norādīja, ka, cik ātri vien iespējams, ir jāpārskata esošais un jāpieņem jauns regulējums.[121]

ICO ziņojums tika publicēts pēc Augstākās tiesas sprieduma lietā, kurā tika izvērtēts, vai Dienvidvelsas policija, izmantojot sejas atpazīšanas sistēmas, nav pārkāpusi cilvēktiesības un datu aizsardzības prasības. Tiesa konstatēja, ka nav ievērotas vairākas prasības, piemēram, policija nebija veikusi saprātīgus pasākumus, lai noskaidrotu, vai programmatūra nerada rasu vai dzimumu aizspriedumus, lai gan tā bija jauna un pretrunīgi vērtēta tehnoloģija. Tajā pašā laikā tā atzina šīs tehnoloģijas izmantošanu par samērīgu un to neaizliedza, kā arī norādīja, ka nav nepieciešams pieņemt jaunu regulējumu, jo attiecībā uz to ir piemērojams esošais regulējums.[122]

Atšķirībā no Apvienotās Karalistes sejas atpazīšanas tehnoloģiju izmantošana policijas darbā ir aizliegta vairākās ASV pilsētās. 2019. gada maijā Sanfrancisko bija pirmā ASV pilsēta, kas aizliedza to izmantot policijas un valsts varas iestādēm. Drīz tai sekoja citas pilsētas – Oklenda, Somervila, Bostona, Kalifornija, Mineapolisa.[123] Visstingrāko aizliegumu ir piemērojusi ASV pilsēta Portlenda Oregonas štatā, kurā 2020. gada septembrī tika aizliegts sejas atpazīšanas tehnoloģijas izmantot gan valsts iestādēm, gan privātajiem uzņēmumiem.[124]

Interesanti, ka pat ASV tehnoloģiju uzņēmumi, kas iepriekš ir mēģinājuši visiem spēkiem izvairīties no saistoša regulējuma, paši ir sākuši pieprasīt šo tehnoloģiju regulējumu. 2020. gadā jūnijā "IBM" un "Amazon" ieviesa ierobežojumus sejas atpazīšanas tehnoloģiju pārdošanai pēc antirasisma protestiem visā pasaulē, reaģējot uz Džordža Floida (*George Floyd*) nāvi.[125] Tam sekoja "Microsoft" paziņojums, ka tas apturēs sejas atpazīšanas tehnoloģiju pārdošanu policijas iestādēm, vismaz līdz brīdim, kad būs pieņemts ASV federālais likums, kas regulēs šīs tehnoloģijas. "Microsoft" prezidents Breds Smits (*Bradford Lee Smith*) paziņoja, ka

121 ICO. (2019). ICO investigation into how the police use facial recognition technology in public places. https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

122 O'Donoghou, C., O'Brien, S. (17 August, 2020). Face-off part 2: UK Court of Appeal finds deficiencies in use of automated facial recognition technology. *Technology Law Dispatch.* https://www.technologylawdispatch.com/2020/08/in-the-courts/face-off-part-2-uk-court-of-appeal-finds-deficiencies-in-use-of-automated-facial-recognition-technology/

123 Lyons (13 February, 2021), Minneapolis prohibits use of facial recognition software ..

124 Peters, J. (9 September 2020). Portland passes strongest facial recognition ban in the US. *The Verge*. https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology

125 Karen, H. (June 12, 2020). The two-year fight to stop Amazon from selling face recognition to the police. *MIT Technology Review.* https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/

visiem tiesību aktiem, kas regulēs sejas atpazīšanu, jābūt stingri balstītiem uz cilvēktiesībām.[126] Tas, ka lielie tehnoloģiju uzņēmumi, kuriem galvenā interese vienmēr ir saistīta ar peļņas gūšanu, sāk pieprasīt no valdībām regulējumu, tiek skaidrots gan ar vēlēšanos novērst riskus, ko rada to tehnoloģijas, un veicināt uzticēšanos, gan ar iespēju tādējādi palielināt savu dominanci. Tajā pašā laikā tie tikai atkārto to, uz ko jau ilgstoši vērš uzmanību pētnieki, tiesību zinātnieki, cilvēktiesību aizstāvji, kā arī starptautiskās organizācijas.

Ne tikai ASV, bet arī ES arvien skaļāk tiek pausts satraukums par šīs tehnoloģijas izmantošanu tiesībaizsardzības iestāžu darbībā, par tās radītajiem būtiskajiem riskiem, kā arī arvien vairāk tiek uzsvērta nepieciešamība regulēt un pat pavisam aizliegt šo tehnoloģiju izmantošanu. Kamēr ES cenšas ātri izstrādāt jaunu mākslīgā intelekta regulējumu, kas noteiktu stingras prasības un ierobežojumus sejas atpazīšanas tehnoloģiju izmantošanai, īpaši aktīvi to pieprasa pilsoniskās sabiedrības organizācijas.

Daudzas cilvēktiesību aizstāvības organizācijas ir vērsušas uzmanību uz šo tehnoloģiju radīto apdraudējumu, arvien skaļāk pieprasot apturēt un aizliegt to izmantošanu. 2020. gada novembrī EDRi uzsāka kampaņu "Atgūsti savu seju!".[127] Divpadsmit cilvēktiesību organizācijas pieprasīja, lai Eiropas valstu iestādes uzklausa iedzīvotājus saistībā ar sejas atpazīšanas un citu biometrisko tehnoloģiju izmantošanu publiskās telpās. EDRi kampaņa aicināja aizliegt biometrisko masveida novērošanu, reaģējot uz tiesībaizsardzības un policijas iestāžu ātru un slepenu nelikumīgu šo tehnoloģiju ieviešanu daudzās Eiropas valstīs. Mēneša laikā tika savākti vairāk nekā 25 000 cilvēku paraksti. 2021. gada februārī EDRi uzsāka arī Eiropas pilsoņu iniciatīvas petīciju, lai aicinātu Eiropas Komisiju aizliegt sabiedriskās vietās izmantot biometriskās novērošanas tehnoloģijas, jo īpaši sejas atpazīšanu.[128] Nedēļas laikā to parakstīja 27 000 ES iedzīvotāju. Šīs iniciatīvas ir rezultāts dažādu valstu cilvēktiesību aizsardzības organizāciju ilgstošiem centieniem iebilst pret sejas atpazīšanas tehnoloģiju izmantošanu masveida novērošanai, tai skaitā protestu un demonstrāciju laikā, tomēr ar to var nepietikt, ja nesekos konkrētas likumdevēja darbības starptautiskā līmenī.

126 Greene, J. (11 June, 2020). Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM. *The Washington Post.* https://www-washingtonpost-com.cdn.ampproject.org/c/s/www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/?outputType=amp

127 SHARE Foundation, Hermes Center, Bits of Freedom, ARTICLE19, Homo Digitalis and EDRi. (12 November, 2020). *EDRi*. Campaign "Reclaim Your Face" calls for a Ban on Biometric Mass Surveillance. https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/

128 European Citizens' Initiative. Civil society initiative for a ban on biometric mass surveillance practices. https://reclaimyourface.eu

Viena no organizācijām, kas piedalās kampaņas rīkošanā, ir Itālijas organizācija "Hermeja centrs" (*Hermes Center*), kas sadarbojās ar "Wired Italia", lai veiktu izmeklēšanu, kuras laikā tika atklāts, ka Komo pilsētā mēnešiem ilgi bija uzstādīta un pārbaudīta sejas atpazīšanas sistēma. Centrs norādīja, ka, uzstādot sistēmu, netika nodrošināta pārredzamība un nebija skaidra tiesiskā regulējuma, kā arī pastāvēja bažas par privāto uzņēmumu lomu, īpaši "Huawei", šo tehnoloģiju ieviešanā. Pilsēta iztērēja valsts naudu sistēmai, kuru Itālijas Datu aizsardzības iestāde lūdza pārtraukt, norādot uz tās neatbilstību pamattiesībām.

EDRi kampaņā iesaistījusies arī Serbijas "SHARE Foundation". Belgradas Republikas laukumā pie sienas stiprinājumiem ir redzamas kupola formas kameras, kas nemanot skenē cilvēkus, kuri staigā pa centrālo laukumu. Tā ir viena no 800 vietām pilsētā, par kuru Serbijas valdība pagājušajā gadā paziņoja, ka to uzraudzīs, izmantojot kameras, kas aprīkotas ar sejas atpazīšanas programmatūru, kura tika iegādāta no Ķīnas uzņēmuma "Huawei". Valdība nejautāja Belgradas iedzīvotājiem, vai viņi šādas kameras vēlas. "SHARE Foundation", kuru vada Danilo Krivokapičs (*Danilo Krivokapic*) pēc neveiksmīgiem informācijas pieprasījumiem, apšaubot projekta likumību un efektivitāti, uzsāka pūļa finansētu sabiedrības kampaņu "Tūkstošiem kameru" (*Hiljade Kamera*), lai atklātu informāciju, identificētu un atzīmētu vietas ap Belgradu, kur tiek uzstādītas viedās novērošanas kameras ar sejas atpazīšanas programmatūru.[129]

Cilvēktiesību aizstāvības organizāciju mērķis ir pēc iespējas plašāk informēt sabiedrību par biometrisko novērošanas tehnoloģiju izmantošanu un to radīto apdraudējumu. Līdzās privātuma zaudēšanai to izmantošana var radīt aizspriedumus un diskrimināciju, kā arī nepamatotu apcietināšanu. Arvien vairāk pētījumu parāda, ka šīs tehnoloģijas nav precīzas un bieži kļūdās, it īpaši, ja tās izmanto attiecībā uz sievietēm, tumšādainiem cilvēkiem, bērniem un veciem cilvēkiem. Tiek arī pamatoti uzsvērts, ka tās ietver biometrisko datu apstrādi, kas rada būtiskus un šobrīd pat skaidri nenosakāmus drošības riskus.[130] Valdības var šīs tehnoloģijas izmantot protestētāju un opozīcijas apspiešanai, ierobežojot vārda, pulcēšanās un biedrošanās brīvību un tādējādi radot būtisku apdraudējumu tiesiskumam un demokrātijai. Šie apdraudējumi detalizētāk apskatīti nodaļas turpinājumā, pirms tam aplūkojot vēl divus mākslīgā intelekta novērošanas tehnoloģiju izmantošanas veidus.

129 Roussi (18 November, 2020), Resisting the rise of facial ..

130 Sk., piemēram, Doffman, Z. (14 August, 2019). New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report. *Forbes.* https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#76f9901046c6

1.2.3. Emociju uztveršanas tehnoloģijas

Mūsdienās ļoti ātri attīstās mākslīgā intelekta tehnoloģijas, kas tiek izmantotas, ne tikai lai atpazītu sejas, bet arī emocijas un dažādas citas īpašības un pazīmes, kas raksturo personas. Tas ir cieši saistīts ar pēdējos gados strauji pieaugošo tendenci izmantot biometriskās tehnoloģijas. Tās pamatā tiek izmantotas personu autentifikācijai jeb identitātes pārbaudei. Biometrisko tehnoloģiju lietošana tiek normalizēta ikdienā. Piemēram, pirkstu nospiedumi vai sejas atpazīšana tiek piedāvāta kā telefonu atbloķēšanas vai bankas maksājumu autentifikācijas līdzeklis. Biometrisko datu izmantošana autentifikācijā ir jānošķir no to izmantošanas citos nolūkos, piemēram, uzvedības analīzei un vērtēšanai, kas rada jaunus būtiskus apdraudējumus.[131]

Ja agrāk tehnoloģijas ļāva atbildēt uz jautājumu, kas ir konkrētais cilvēks, tad tagad jau tiek uzdots jautājums, kāds ir šis cilvēks?[132] Līdzās personu identificēšanai arvien vairāk tiek apgalvots, ka mākslīgā intelekta sistēmas no ķermeņa datiem spēj izsecināt demogrāfiskās īpašības, emocionālos stāvokļus un personības iezīmes. Mākslīgā intelekta sistēmas, piemēram, sejas atpazīšanas tehnoloģijas, arvien vairāk izmanto algoritmus, kas analizē emocijas, uzvedību, balsi, izteicienus, acu kustības, gaitu, ķermeņa reakciju u. tml.

Emociju uztveršanas sistēma ir mākslīgā intelekta sistēma, kuras mērķis ir identificēt vai izsecināt fizisku personu emocijas vai nodomus, pamatojoties uz viņu biometriskajiem datiem.[133] Emocionālais mākslīgais intelekts attiecas uz tehnoloģijām, kuras izmanto afektīvās skaitļošanas un mākslīgā intelekta metodes, lai nojaustu, uzzinātu un mijiedarbotos ar cilvēka emocionālo dzīvi.[134] Šīs tehnoloģijas tiek sauktas arī par uzvedības atpazīšanas (*behavior recognision* – angļu val.) tehnoloģijām.

Izšķir arī biometriskās kategorizācijas sistēmas, kas ir mākslīgā intelekta sistēmas, kuru mērķis ir noteikt fizisku personu piederību noteiktām kategorijām, piemēram, tādām kā dzimums, vecums, matu krāsa, acu krāsa, tetovējumi, etniskā izcelsme vai seksuālā vai politiskā orientācija, pamatojoties uz biometriskajiem datiem.[135]

Daudzi zinātnieki populārzinātniskās grāmatās ir norādījuši, ka mākslīgā intelekta un biotehnoloģiju saplūšana ir viens no nozīmīgākajiem nākotnes

131 Pauwels, E. (2020). Artificial Intelligence and data capture technologies in violence and conflict prevention. https://www.globalcenter.org/wp-content/uploads/2020/10/GCCS_AIData_PB_H.pdf

132 Kak, A. (ed.). (2020). *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute. https://ainowinstitute.org/regulatingbiometrics.html

133 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts, 3. panta 34. punkts.

134 Mcstay (2020), Emotional AI, Soft Biometrics and the Surveillance ..

135 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts, 3. panta 35. punkts.

izaicinājumiem cilvēcei. Zinātnieks Stīvens Hokings (*Stephen Hawking*) grāmatā "Īsas atbildes uz svarīgiem jautājumiem" (*Brief Answers to the Big Questions*), kuru gan viņš pats nepaguva pabeigt un kura tika publicēta jau pēc viņa nāves 2018. gadā, atzīst, ka jaunu tehnoloģiju, īpaši mākslīgā intelekta un biotehnoloģiju, attīstība rada jaunus pamattiesību riskus un apdraud demokrātiju.[136] Arī vēsturnieks un filozofs profesors Juvāls Noa Harari (*Yuval Noah Harari*) grāmatā "21 lekcija 21. gadsimtam" (*21 Lessons for the 21st century*) brīdina, ka informācijas tehnoloģiju un biotehnoloģiju revolūcija un saplūšana, kas ļauj lielo datu algoritmiem izprast mūsu domas un jūtas, tās kontrolēt un ar tām manipulēt, rada lielāko izaicinājumu, ko cilvēce ir jebkad piedzīvojusi.[137] Pēc Harari domām, iespējams, visbūtiskākā 21. gadsimta attīstības tendence ir "zem ādas" uzraudzība, kura rada iespēju pilnīgi izprast cilvēku, ievācot biometriskos datus un tos analizējot, un var ļaut uzzināt par cilvēku vairāk, nekā viņš zina pats par sevi.[138] Ja iepriekš valdības un uzņēmumi galvenokārt novēroja mūsu rīcību pasaulē – kur dodamies, ar ko satiekamies –, tad tagad tos vairāk interesē tas, kas notiek mūsu ķermenī – mūsu veselības stāvoklis, ķermeņa temperatūra un asinsspiediens. Šāda veida biometriskā informācija var atklāt par mums daudz vairāk nekā jebkad agrāk. Zinātnieks turklāt brīdina, ka Covid-19 pandēmija var būt nozīmīgs pagrieziena punkts novērošanas vēsturē, jo tā var "normalizēt" masveida novērošanas rīku ieviešanu valstīs, kuras līdz šim tos ir noraidījušas, kā arī tā liecina par dramatisku pāreju no "virs ādas" uz "zem ādas" novērošanu.[139]

Mākslīgā intelekta sistēmu izmantošana fizisku personu emocionālā stāvokļa noteikšanai apdraud cilvēktiesības un var radīt nozīmīgu kaitējumu indivīdiem. Tās tiek arvien plašāk izmantotas personu vērtēšanai dažādās jomās, ieskaitot izglītību un darba attiecības. Tās tiek izmantotas skolās, lai izvērtētu skolēnu sasniegumus. Tās tiek izmantotas darba intervijās un darbinieku vērtēšanā, lai noteiktu, kurš ir "produktīvāks" vai "labāks darbinieks", turklāt bieži vien pašus darbiniekus par to neinformējot.[140] ASV bankas izmanto šīs tehnoloģijas, lai varētu novērtēt, vai darbinieki pietiekami bieži smaida bankas apmeklētājiem.[141] Tehnoloģiju uzņēmumi nāk klajā ar arvien jaunām novērošanas ierīcēm, kas

136 Hawking, S. (2018). *Brief Answers to the Big Questions*. United States: Bantam, p. 186.

137 Harari, Y. N. (2018). *21 Lessons for the 21st Century*. New York: Spiegel & Grau.

138 Harari, Y. N. (20 March, 2020). Yuval Noah Harari: the world after coronavirus. *Financial Times* https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

139 Harari, Y. N. (2020). Yuval Noah Harari: "Every crisis is also an opportunity." *UNESCO Courier*, 2020-3. https://en.unesco.org/courier/2020-3/yuval-noah-harari-every-crisis-also-opportunity

140 Sk. Crawford, et al. (2019), AI Now 2019 Report.

141 Paresh, D., Jeffrey, D. (19 April, 2021). U.S. banks deploy AI to monitor customers, workers amid tech backlash. *Reuters.* https://www.reuters.com/technology/us-banks-deploy-ai-monitor-customers-workers-amid-tech-backlash-2021-04-19/

ļauj iegūt un analizēt lietotāju biometriskos datus. "Amazon" veselības aprocei "Halo" ir paredzēta izvēles funkcija, kas prasa, lai aproces lietotājs nofotografētu četras ķermeņa puses apakšveļā vai ādas drēbēs, un pēc tam tā ģenerē ķermeņa 3D modeli, kā arī izmanto mikrofonu un mašīnmācīšanos, lai analizētu lietotāja balsi, sniedzot ieskatu par to, kā cilvēki uztver lietotāja toni, piemēram, vai tas ir valdonīgs vai aizkaitināts.[142] Šo ierīču spējas ir ļoti ierobežotas, un to rezultāti nav ticami, taču tas ir labs veids, kādā uzņēmumi var iegūt visintīmākos datus un attīstīt savas tehnoloģijas tālāk.

Būtisku apdraudējumu rada novērošanas tehnoloģiju izmantošana arī valsts iestādēs. Piemēram, Kortreikā Beļģijā un Marveljā Spānijā vietējā policija izmantoja ķermeņa atpazīšanas tehnoloģiju, kas analizē personu gaitu un apģērbu. Tā ļauj arī atpazīt sejas, tomēr, lai šo funkciju ieslēgtu, tika gaidīta "zaļā gaisma" no uzraugošajām iestādēm.[143]

Plašu kritiku izraisīja ES finansētais projekts "iBorderCtrl", kas tika īstenots no 2016. līdz 2019. gadam. Tā mērķis bija izstrādāt automatizētu melu noteikšanas sistēmu, lai uzlabotu ES robežu kontroli. Projektā iesaistījās Ungārijas, Grieķijas, kā arī Latvijas drošības iestādes. Projekts paredzēja ieviest ieceļotāju kontroles sistēmu, kas darbotos šādi – ieceļotājs, kurš vēlas iekļūt ES, pirms ierašanās lidostā, izmantojot savu datoru, piesakās vietnē, augšupielādējot savas pases attēlu. Uz ekrāna parādās virtuāls policists tumši zilā formas tērpā. Viņš uzdod dažādus jautājumus, piemēram: "Kāds ir tavs uzvārds?", "Kāda ir tava pilsonība?", "Kāds ir tavs ceļojuma mērķis?" Ieceļotājs atbild uz uzdotajiem jautājumiem, un virtuālais policists izmanto tīmekļa kameru, lai skenētu viņa seju un acu kustības, lai noteiktu, vai tiek melots vai nē. Intervijas beigās sistēma piešķir kvadrātkodu, kas jāuzrāda apsargam robežkontrolē. Apsargs noskenē kodu, izmantojot planšetdatoru, noņem pirkstu nospiedumus un pārskata uzņemto sejas attēlu, lai pārbaudītu, vai tas atbilst pasei. Apsarga planšetdatorā tiek parādīts rezultāts 100 punktu skalā, kas parāda, vai mašīna ir atzinusi sacīto par patiesību. Ceļotājiem, kurus uzskata par bīstamiem, var liegt ieceļošanu ES.[144] Eiropas datu aizsardzības biju-šais uzraudzītājs Džovanni Butarelli (*Giovanni Buttarelli*) vērsa uzmanību uz to, ka šī sistēma var diskriminēt cilvēkus viņu etniskās izcelsmes dēļ. Šāda veida sistēmas būtiski apdraud cilvēktiesības, īpaši diskriminācijas aizlieguma principu.

EDRi vērš uzmanību, ka mākslīgā intelekta testēšanai uz Eiropas robežām, lai it kā atklātu melus, izmantojot imigrācijas lietotnes, vai maldināšanu par angļu valodas testiem, izmantojot balss analīzi, trūkst ticama zinātniska pamatojuma.

142 Swisher, K. (27 November, 2020). Amazon wants to get even closer. Skintight. *The New York Times.* https://www.nytimes.com/2020/11/27/opinion/amazon-halo-surveillance.html

143 Kayser-Bril (18 June, 2020), At least 11 police forces use face recognition ..

144 Gallagher, Jona (26 July, 2019), We tested Europe's new lie detector for travelers ..

ES migrācijas politikā arvien lielāku nozīmi ieņem mākslīgā intelekta sistēmas, piemēram, sejas atpazīšana, algoritmiskās profilēšanas un prognozēšanas rīki, kas paredzēti izmantošanai migrācijas pārvaldības procesos, tostarp piespiedu izraidīšanai. Šie izmantošanas gadījumi var pārkāpt datu aizsardzības tiesības, tiesības uz privātumu, tiesības uz nediskrimināciju un vairākus starptautisko migrācijas tiesību principus, tostarp tiesības meklēt patvērumu.[145]

Kā norāda AI HLEG, mākslīgā intelekta tehnoloģiju izmantošana personu vērtēšanā rada būtisku pamattiesību apdraudējumu: "Jebkāda iedzīvotāju vērtēšana var novest pie patstāvības zaudējuma un apdraudēt nediskriminēšanas principu. Vērtēšana būtu jāizmanto tikai tad, ja tā ir pamatota un ja pasākumi ir samērīgi un taisnīgi. Valsts iestāžu vai privātā sektora veikta iedzīvotāju vērtēšana (vispārējs "morālās personības" vai "ētiskās godprātības" vērtējums) visos aspektos un plašā mērogā apdraud šīs vērtības, jo īpaši, ja to neizmanto saskaņā ar pamattiesībām vai ja to izmanto nesamērīgi, bez skaidri noteikta un paziņota leģitīmā mērķa. [..] Vēlams, lai, kad vien tas iespējams, tiktu piedāvāta iespēja izstāties no vērtēšanas mehānisma bez nelabvēlīgām sekām; citos gadījumos ir jāparedz vērtējuma apstrīdēšanas un labošanas iespējas. Tas ir īpaši svarīgi situācijās, kad pušu starpā pastāv varas asimetrija. Šādas atteikšanās iespējas ir jānodrošina tehnoloģijas izstrādes stadijā, kad tas ir vajadzīgs, lai garantētu atbilstību pamattiesībām, un ir nepieciešams demokrātiskā sabiedrībā."[146]

Mākslīgā intelekta tehnoloģiju izmantošana cilvēku vērtēšanai un uzvedības analizēšanai ir radījusi plašu kritiku ne tikai tāpēc, ka tā var atspoguļot dažādus aizspriedumus un būt diskriminējoša, bet arī tāpēc, ka trūkst zinātnisku pierādījumu, vai šādas tehnoloģijas var nodrošināt precīzus vai pat derīgus rezultātus. Ir apstrīdams zinātniskais pamats tehnoloģijām, kas apgalvo, ka, pamatojoties uz fizioloģiskiem mērījumiem, piemēram, sejas izteiksmi, balsi un gaitu, var atklāt tādas lietas kā personība, emocijas, garīgā veselība un citus iekšējos stāvokļus. Tāpēc tām nevajadzētu būt nozīmīgām svarīgu lēmumu pieņemšanā par cilvēka dzīvi, piemēram, darbinieku izvērtēšanā vai pieņemšanā darbā, apdrošināšanas cenu noteikšanā, pacientu sāpju novērtēšanā vai skolā skolēnu sasniegumu izvērtēšanā. Pilsoniskās sabiedrības organizācijas un zinātniskās institūcijas, piemēram, *AI Now* institūts, arvien skaļāk un pārliecinošāk mudina valdības aizliegt šo tehnoloģiju izmantošanu, īpaši tādu svarīgu lēmumu pieņemšanā, kas ietekmē cilvēku dzīvi un piekļuvi iespējām.[147]

145 EDRi (12 January, 2021), Re: Open letter: Civil society call for the introduction of red lines ..

146 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

147 Crawford, et al. (2019), AI Now 2019 Report.

Būtisku apdraudējumu rada arī šāda veida mākslīgā intelekta novērošanas tehnoloģiju izmantošana tiesībaizsardzības iestāžu un policijas darbā noziedzības prognozēšanai.

1.2.4. Prognozēšana tiesībaizsardzības nolūkā

Prognozēšana tiesībaizsardzības nolūkā (*predictive policing* – angļu val.) ir apzīmējums, kas balstās uz apgalvojumu, ka, izmantojot datu kopu algoritmisku apstrādi, var atklāt iespējamo likumpārkāpumu modeļus nākotnē, kurus tādējādi var novērst, pirms tie tiek īstenoti.[148] Lai gan prognozējošās tiesībaizsardzības pirmsākumi varētu būt meklējami datorizētas noziedzības kontroles eksperimentos 20. gadsimta 70. gados un prognozēšana noziedzības un soda jomā ir izstrādāta un apspriesta daudzus gadu desmitus, šis termins galu galā tika saistīts tieši ar lielajiem datiem.[149] Prognozēšana kā plaša tendence ir ievērojami ietekmējusi drošības jomas attīstību visā pasaulē, tai skaitā Eiropā un ASV.

Prognozēšanas metodes tiesībaizsardzības nolūkos var iedalīt četrās lielās kategorijās:

1) metodes, kuru mērķis ir prognozēt noziedzīgus nodarījumus vai prognozēt, kur un kad ir paaugstināts noziedzības risks;
2) metodes, kuru mērķis ir prognozēt likumpārkāpējus vai identificēt personas, kuras nākotnē var izdarīt likumpārkāpumu vai atkārtotu pārkāpumu;
3) metodes, kuru mērķis ir prognozēt vai izveidot profilus, kas ir līdzīgi iepriekšējo likumpārkāpēju profiliem, un
4) metodes, kuru mērķis ir prognozēt noziedzīgu nodarījumu upurus, lai identificētu grupas vai personas, kuras varētu kļūt par noziedzīga nodarījuma upuriem.[150]

Prognozēšanas metodes var iedalīt, balstoties arī uz algoritmisko datu vai izlūkošanas analīzes iespējamiem mērķiem tiesībaizsardzības iestāžu un policijas darbības kontekstā. Proti, ir iespējams izšķirt prognozēšanu tiesībaizsardzības nolūkos, kas iekļauj stratēģisko plānošanu, prioritāšu noteikšanu un prognozēšanu; operatīvās izlūkošanas sasaisti un novērtēšanu, kas savukārt var ietvert,

148 Wilson, D. (2018). Algorithmic patrol: the futures of predictive policing, p. 108. In: Zavrsnik, A. (ed.), *Big Data, Crime and Social Control. Routledge Frontiers of Criminal Justice*. Routledge, London, p. 108; sk. arī Gonzelez Fuster, G. (2020). Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf

149 Wilson (2018), Algorithmic patrol: the futures of predictive policing, p. 109.

150 Perry, W. L. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND.

piemēram, noziedzības novēršanas darbības, lēmumu pieņemšanu vai riska novērtēšanu attiecībā uz indivīdiem.[151]

Prognozējošā pieeja tiesībaizsardzībā bieži vien vismaz daļēji balstās uz tādu datu apstrādi, kas sākotnēji nav saistīti ar noziedzību, bet ko vāc privātie uzņēmumi, piemēram, banku, telekomunikāciju, tūrisma jomā. Plaši izmantota metode ir sociālo tīklu analīze. Prognozēšanas shēmas parasti balstās uz privātu uzņēmumu ražotu programmatūru neatkarīgi no tā, vai tie ir uzņēmumi, kas specializējas šajā jomā, vai lielie tehnoloģiju uzņēmumi.[152]

Arvien lielāku popularitāti iegūst prognozēšanas metodes, kas balstās uz sejas atpazīšanas tehnoloģijām sabiedrisko vietu uzraudzībai un analizē un vērtē cilvēku uzvedību, proti, mēģina atklāt aizdomīgu vai neparastu uzvedību. Balstoties uz datu plūsmu daudzveidību, mākslīgā intelekta sistēmas var tikt izmantotas, lai automatizētu anomāliju noteikšanu un veiktu uzvedības analīzi vai atrastu modeļus un anomālijas pamatdatos par indivīdu un iedzīvotāju uzvedību. Biometriskās identifikācijas sistēmas arvien vairāk tiek izmantotas iedzīvotāju profilēšanai, analizējot, kā cilvēki dzīvo, pārvietojas un jūtas.

Arvien biežāk tiek apgalvots, ka mākslīgā intelekta sistēmas var iemācīties interpretēt un paredzēt cilvēku rīcību, kā arī klasificēt emocijas un noteikt uzvedību kā "normālu", "nenormālu" vai "kaitīgu". Viens no argumentiem, lai veiktu šādu uzvedības analīzi, tiek minēts, ka tā var sniegt būtiskus ieguvumus, īpaši drošībai. Predikatīvās jeb paredzošās uzvedības analīzes un iedzīvotāju datu saglabāšanas (*data capturing* – angļu val.) jaunā paradigma tiek saskatīta kā risinājums humānās palīdzības, konfliktu novēršanas, miera un drošības izaicinājumiem. Tiek publicēti pētījumi, kas cenšas parādīt, ka mākslīgā intelekta un datu uztveršanas tehnoloģiju saplūšana var būtiski ietekmēt mainīgo konfliktu raksturu un pasaules drošību, tostarp saistībā ar vardarbīgu ekstrēmismu un terorismu. Tehnoloģiskā saplūšana un divējāda lietojuma sistēmu izmantošana sniedz iespējas mērķtiecīgi novērot personu un iedzīvotāju uzvedību, kā arī veikt automatizētu un prognozējošu uzvedības un situācijas analīzi, piemēram, apkopojot lielu daudzumu uzvedības un konteksta informācijas par iedzīvotājiem, kuri dzīvo nestabilās valstīs, vai par personām, kurām ir tendence uz vardarbīgu uzvedību. Tiek norādīts, ka ANO aģentūras un humānās palīdzības sniedzēji aizvien vairāk paļaujas uz digitālo platformu un privātā sektora vadošo uzņēmumu iespējām mākslīgā intelekta, prognozējošās datu analīzes un biometrisko identitātes pārvaldības sistēmu jomā, un mākslīgā intelekta un datu uztveršanas tehnoloģijas pakāpeniski ieņem arvien nozīmīgāku lomu vardarbības un konfliktu novēršanā.[153]

151 Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement.

152 Wilson (2018), Algorithmic patrol: the futures of predictive policing, p. 114.

153 Pauwels (2020), Artificial Intelligence and data capture technologies ..

Tajā pašā laikā mākslīgā intelekta un datu uztveršanas tehnoloģijas var izmantot arī prettiesiskiem mērķiem. Šīs tehnoloģijas tiek sauktas arī par divējāda lietojuma tehnoloģijām (*dual-use technologies* – angļu val.), ņemot vērā, ka tās var izmantot gan civiliem, gan militāriem mērķiem. Valstis, korporācijas, kā arī vardarbīgi nevalstiski dalībnieki tās var izmantot ļaunprātīgi, lai veiktu precīzu novērošanu.

Līdz šim nav pierādījumu, ka datu iegūšanas tehnikas, kas tiek izmantotas uzraudzībai, ir efektīvs līdzeklis, lai cīnītos pret teroristiem. Tajā pašā laikā tās ir daudz vairāk piemērotas citiem mērķiem, piemēram, sociālajai kontrolei, manipulēšanai, diskriminēšanai un pat digitālās diktatūras radīšanai.[154] Tam visspilgtākais piemērs ir Ķīna, kur mākslīgā intelekta novērošanas tehnoloģijas tiek patvaļīgi un prettiesiski izmantotas, lai kontrolētu iedzīvotājus.[155]

Ķīna ir ieviesusi un turpina attīstīt augsto tehnoloģiju novērošanas sistēmas, kas balstās uz sejas atpazīšanu un mākslīgo intelektu, lai kontrolētu tās 1,4 miljardus iedzīvotāju. Ķīnā tiek ieviesta tā sauktā "sociālā kredīta" sistēma, kas katram iedzīvotājam piešķir personisko rezultātu rādītāju. Uzraudzības sistēma ļauj kontrolēt visus iedzīvotāju personiskās dzīves aspektus, piešķirot vai atņemot punktus par pašu niecīgāko pārkāpumu. Piemēram, punkti var tikt noņemti par skaļas mūzikas klausīšanos un smēķēšanu neatļautā vietā. Ja personai ir augsts sociālais kredīts, proti, ja uzvedība ir "pareiza", tiek piešķirtas dažāda veida privilēģijas, piemēram, iespēja saņemt labus veselības aprūpes pakalpojumus, rezervēt labākās viesnīcas, nopirkt lētus lidojumus, iegūt lētus aizdevumus, tikt uzņemtam labākajās universitātēs un viegli atrast darbu. Savukārt citi, kam ir zems punktu skaits, tiek izraidīti no sabiedrības. Viņiem ir aizliegts ceļot, nav ļauts atrasties labākajās viesnīcās, saņemt kredītu, strādāt valsts iestādēs, viņi paši vai viņu bērni nevar studēt labākajās universitātēs, viņiem pat var atņemt mājdzīvnieku, kā arī publiski nosaukt par sliktu pilsoni. 2018. gadā Ķīna publicēja pilsoņu vārdus un pārkāpumus, kādus viņi izdarījuši, piemēram, kā pārkāpums tika norādīts mēģinājums caur lidostas drošības pārbaudi ienest šķiltavas. Tiesību aizstāvji ir atklājuši, ka Ķīnas valdība uzsāka uiguru novērošanu, izmantojot sejas atpazīšanu un biometrisko datu, tostarp DNS paraugu un balss paraugu, analīzi, lai prognozētu aizdomīgu uzvedību. Ķīnas varas iestādes ir izveidojušas plašu sejas atpazīšanas algoritmu sistēmu, kas ir apmācīta noteikt ādas toņus un sejas vaibstus, kas raksturīgi uiguru etniskajai piederībai. Šāda veida profilēšana padara

154 Schneier, B. (2016). *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World.* New York, London: W. W. Norton & Company, pp. 159–164.

155 Sk., piemēram, Carney, M. (17 September, 2018). Leave no dark corner. *ABC.* http://mobile.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278?pfmredir=sm&sf197878142=1&smid=Page:%20ABC%20Australia-Facebook_Organic&WT.tsrc=Facebook_Organic

Ķīnu par vadošo valsti, kas prettiesiski izmanto mākslīgo intelektu, lai uzraudzītu etniskās grupas un potenciāli varētu arī eksportēt jauna veida automatizētas rasu novērošanas tehnoloģijas.[156]

Mākslīgā intelekta novērošanas sistēmu izmantošana vismaz dažās pasaules vietās var novest pie tā, ka beidz pastāvēt sabiedrība, kuru veido brīvi autonomi pilsoņi, kuri paši izvēlas un rīkojas, pamatojoties uz brīvo gribu. Brīvā sabiedrībā pilsoņiem ir atstāta zināma rīcības brīvība starp to, kādi ir noteikumi un kas ir jāizpilda. Cilvēkiem ir atļauts "atbrīvoties" no nelieliem pārkāpumiem, tāpēc ka labi funkcionējošā sabiedrībā vairākums cilvēku lielāko daļu laika paši vēlas ievērot likumus. Uzraudzības sistēmas, kas nodrošina konkrētu likumu ievērošanu, savukārt nepieļauj izņēmumus, līdzīgi kā tos nepieļauj, piemēram, fotoradaru sistēma ceļu satiksmes pārkāpumu fiksēšanai. Arī valstīs, kurās pastāv absolūta iedzīvotāju kontrole, nekāda atkāpšanās no noteikumu neievērošanas nav pieļaujama.

Lai arī Eiropas valstīs nepastāv sociālā vērtēšanas sistēma un absolūta uz tehnoloģijām balstīta iedzīvotāju kontroles sistēma, tomēr arvien vairāk tiek izmantotas mākslīgā intelekta novērošanas tehnoloģijas, to skaitā personu vērtēšanai un uzvedības analīzei. Šī tendence ir ievērojami palielinājusies Covid-19 pandēmijas laikā.

1.2.5. Jauno novērošanas tehnoloģiju plūdi cīņā ar Covid-19

2020. gads iezīmēja strauju pagriezienu digitālo novērošanas tehnoloģiju izmantošanā. Covid-19 pandēmija radīja vēl nebijušus izaicinājumus veselības aprūpes sistēmām, kā arī dramatiskas sociālekonomiskās sekas visā pasaulē. Valstis ar lielu steigu meklēja inovatīvus veidus, kā uz datiem balstītas tehnoloģijas varētu izmantot pandēmijas ierobežošanai. Pasaule saskārās ar jaunu novērošanas tehnoloģiju plūdiem, kas tika strauji izstrādātas un ieviestas, lai labāk izprastu Covid-19 pandēmiju un cīnītos ar tās izplatību, radot jaunus izaicinājumus datu aizsardzībai un privātumam.

Esošās un jaunās digitālās tehnoloģijas tika izmantotas, lai papildinātu tradicionālos pasākumus, piemēram, sociālo distancēšanos un testēšanu, ar mērķi uzlabot to efektivitāti, lai veiktu novērošanu, tai skaitā reālā laikā, kā individuālā, tā arī sabiedrības līmenī.

Vairākas valstis salīdzinoši ātri ieviesa tehnoloģiskus risinājumus, lai palīdzētu reaģēt uz koronavīrusu un sasniegt piecus galvenos mērķus. Tie ir:

156 Wakefield, J. (26 May, 2021). AI emotion-detection software tested on Uyghurs. *BBC News.* https://www.bbc.com/news/technology-57101248; Article 19. (2021). Emotional Entanglement: China's emotion recognition market and its implications for human rights. https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf

1) karantīnas ievērošana un pārvietošanās atļaušana, lai uzzinātu, vai cilvēki atrodas tur, kur viņiem vajadzētu atrasties, vai lai atļautu pārvietoties tiem, kas nav inficēti;
2) kontaktu izsekošana, lai uzzinātu, kuri cilvēki ir bijuši saskarsmē;
3) modeļa un plūsmas modelēšana, lai noskaidrotu slimības vietu un izplatību un to, cik daudz cilvēku ir bijuši konkrētā vietā;
4) sociālās distancēšanās un pārvietošanās uzraudzība, lai zinātu, vai cilvēki ievēro ieteicamo drošo attālumu un pārvietošanās ierobežojumus;
5) simptomu izsekošana, lai zinātu, vai iedzīvotājiem ir kādi slimības simptomi.[157]

Viens no digitālajiem risinājumiem, kas tika strauji izstrādāts un ieviests, ir mobilo telefonu lietotnes. Tās tika ieviestas visā pasaulē – Ķīnā, Dienvidkorejā, Singapūrā, Izraēlā, Taivānā, Austrālijā, ASV, kā arī lielākajā daļā ES valstu. Lai gan vairākums valstu mobilās lietotnes ieviesa kontaktu fiksēšanai un izsekošanai, tomēr tās tika izveidotas arī daudziem citiem mērķiem: lai sniegtu informāciju; lai sniegtu jaunākās ziņas, brīdinātu un sniegtu instrukcijas iedzīvotājiem; lai sniegtu medicīnisko atbalstu; lai iedzīvotāji varētu paši diagnosticēt vai ziņot par saslimšanu; sabiedrības kontrolei, t. i., gan brīvprātīgas, gan piespiedu lietotnes karantīnas ievērošanas kontrolei un pārvietošanās kontrolei; lai informētu par pārkāpumiem.[158]

Ieviest tehnoloģiju risinājumus cīņā ar pandēmiju mudināja daudzas starptautiskas organizācijas. Divas dienas pēc Covid-19 pasludināšanas par pandēmiju, 2020. gada 13. martā, Pasaules Veselības organizācija aicināja valstis kopā ar testēšanu, sociālo distancēšanos un citiem pasākumiem izsekot kontaktus, lai novērstu infekcijas un glābtu dzīvības.[159]

Anonimizētu mobilitātes datu izmantošana un kontaktu izsekošana, izmantojot mobilās lietotnes, bija pirmā ES valstu kopīgā un koordinētā atbildes reakcija uz Covid-19 pandēmiju. 2020. gada 8. aprīlī Eiropas Komisija pieņēma ieteikumu, lai izstrādātu kopīgu pieeju, sauktu par rīkkopu, lai krīzes pārvarēšanā izmantotu digitālus līdzekļus, it īpaši mobilās lietotnes un anonimizētus datus par

157 Countries are using apps and data networks to keep tabs on the pandemic. (26 March, 2020). *The Economist.* https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic; sk. arī Whitelaw, S., Mamas, A., Topol, E., van Spall, H. G. C. (2020). Applications of Digital Technology in COVID-19 Pandemic Planning and Response. *The Lancet Digital Health,* 2(8). https://doi.org/10.1016/S2589-7500(20)30142-4.

158 Council of Europe. (2020). Digital Solutions to fight COVID-19. 2020 Data Protection Report. https://rm.coe.int/report-dp-2020-en/16809fe49c

159 WHO. (13 March, 2020). WHO Director-General's opening remarks at the media briefing on COVID-19 – 13 March 2020. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing--14-september-2022

iedzīvotāju mobilitāti.[160] 2020. gada 15. aprīlī Eiropadome un Eiropas Komisija pieņēma kopīgo Eiropas ceļvedi, uzsverot, ka ES veic pasākumus, lai atbalstītu kontaktu izsekošanas lietotnes, kā arī apkopotu un anonimizētu datu apstrādi no sociālo mediju un mobilo tīklu operatoriem kā papildu pasākumus, kas palīdzētu atcelt pulcēšanās, ceļošanas un cita veida ierobežojumus.[161] Dokumentos norādīts, ka anonimizētu atrašanās vietu un kustības datu apstrāde no mobilajiem telefoniem un sociālo mediju lietotnēm var palīdzēt cīņā ar pandēmiju, jo šāda apstrāde var atklāt sociālās mobilitātes modeļus un tendences un var izrādīties noderīga vīrusa izplatības prognozēm.

Plašas diskusijas izraisīja kontaktu izsekošanas lietotnes. Visu šo lietotņu mērķis ir retrospektīvi izsekot un brīdināt apstiprināto inficēto personu kontaktpersonas. Tomēr valstis izvēlējās dažādas pieejas, kā ieviest šīs lietotnes, un dažas valstis, piemēram, Norvēģija[162] un Lietuva[163], kas pirmās steidzās tās ieviest, vēlāk bija spiestas tās apturēt privātuma pārkāpumu dēļ.

2021. gada 17. martā Eiropas Komisija publicēja priekšlikumu regulai par digitālā zaļā sertifikāta ieviešanu, lai atvieglotu brīvu pārvietošanos Covid-19 pandēmijas laikā.[164] Ideja par vakcinācijas sertifikātu ieviešanu ātri tika īstenota daudzās Eiropas un pasaules valstīs, vienlaikus izraisot plašas diskusijas, it īpaši par to atbilstību vienlīdzības un nediskriminācijas principiem.[165] Dānija kļuva par pirmo Eiropas valsti, kas 2021. gada aprīlī ieviesa vakcīnas sertifikātus un

160 Komisijas Ieteikums (ES) 2020/518 (2020. gada 8. aprīlis) par vienotu Savienības rīkkopu tehnoloģiju un datu izmantošanai ar mērķi apkarot Covid-19 krīzi un iziet no tās, it īpaši attiecībā uz mobilajām lietotnēm un anonimizētu mobilitātes datu izmantošanu. *OV L* 114/7, 14.04.2020.

161 Eiropadome un Eiropas Komisija. (2020). Kopīgais Eiropas ceļvedis Covid-19 ierobežošanas pasākumu atcelšanai. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020XC0417(06)&from=EN

162 Manancourt, V. (15 June, 2020). Norway suspends contact-tracing app over privacy concerns. *POLITICO.* https://www.politico.eu/article/norway-suspends-contact-tracing-app-over-privacy-concerns/

163 Pugh, A. (28 May, 2020). Lithuanian contact tracing app suspended. *Global Data Review.* https://globaldatareview.com/coronavirus/lithuanian-contact-tracing-app-suspended

164 Eiropas Komisija. (2021). Priekšlikums. Eiropas Parlamenta un Padomes regula par sadarbspējīgu vakcinācijas, testēšanas un pārslimošanas sertifikātu izdošanas, verifikācijas un akceptēšanas satvaru nolūkā atvieglot brīvu pārvietošanos Covid-19 pandēmijas laikā (digitālais zaļais sertifikāts). https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52021PC0130&from=EN

165 Sk., piemēram, EDPB, EDPS. (2021). EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate). https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042021-proposal_en

izmantoja tos restorānos, bāros, pat universitātēs. Latvijā digitālie Covid-19 sertifikāti tika ieviesti 2021. gada jūnijā un izmantoti, lai varētu apmeklēt izklaides un sporta pasākumus, piemēram, pasaules hokeja čempionāta spēles, teātrus, koncertus, kafejnīcas iekštelpās, bet vēlāk arī lai ierobežotu nevakcinēto personu iespējas mācīties un strādāt. Šāda digitālo sertifikātu izmantošana radīja daudzus jautājumus par to samērīgumu un atbilstību cilvēktiesībām, un tie nonāca arī līdz tiesai.[166]

Valstis izmantoja arī cita veida tehnoloģijas, lai ierobežotu pandēmijas izplatību, to skaitā mobilās un biometriskās lietotnes, elektroniskās aproces un citas biometriskās valkājamās ierīces, termālās kameras, kā arī attālinātu novērošanu ar droniem un robotiem.[167] Tālāk sniegti daži piemēri, lai parādītu uzraudzības tehnoloģiju ieviešanu dažādās pasaules valstīs.

Ķīnā valsts iestādes iedzīvotājiem uzlika pienākumu augšupielādēt mobilo lietotni un skenēt kvadrātkodu pie ieejas institūcijās, lai pārbaudītu personas infekcijas statusu un atļautu tai iekļūt iepirkšanās centros, metro un citās sabiedriskās vietās, un šī lietotne nosūta brīdinājumu vietējai policijai, ja personai ir jāatrodas karantīnā un tā nedrīkst atrasties ārpus dzīvesvietas.[168]

Līdzīgi Krievijā, Maskavā, valsts iestādes ieviesa lietotņu sistēmu, lai iedzīvotājiem apstiprinātu braucienus pa izvēlēto maršrutu un ieviestu karantīnu. Reģistrējoties sistēmā, personai vajadzēja sasaistīt savu mobilo telefonu ar pilsētas e-pārvaldes sistēmu un augšuplādēt personas apliecību, informāciju par darba devēju un transportlīdzekļa numura zīmi.[169] Krievijā un Moldovā, lai kontrolētu karantīnas ievērošanu, tika izmantotas arī sejas atpazīšanas tehnoloģijas.[170]

Taivānā tika ieviesta obligāta tālruņa atrašanās vietas izsekošanas sistēma, lai nodrošinātu karantīnu. Iedzīvotājiem, kuriem nebija savu telefonu, tika izsniegti

166 Sk., piemēram, Satversmes tiesas 2022. gada 18. februāra lēmums lietā Nr.2021-10-03.

167 Sk., piemēram, Vargo, D., et al. (2021). Digital Technology Use during COVID-19 Pandemic: A Rapid Review. *Human Behavior and Emerging Technologies,* 3(1), pp. 13–24. https://doi.org/10.1002/hbe2.242; Kitchin, R. (2020). Civil Liberties or Public Health, or Civil Liberties and Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19. *Space and Polity*, 24(3), pp. 362–381. https://doi.org/10.1080/13562576.2020.1770587; Couch, Robinson, Komesaroff (2020), COVID-19 – Extending Surveillance ..

168 Goh, B. (26 February, 2020). China rolls out fresh data collection campaign to combat coronavirus. *Reuters.* https://www.reuters.com/article/us-china-health-data-collection/china-rolls-out-fresh-data-collection-campaign-to-combat-coronavirus-idUSKCN20K0LW

169 Ilyushina, M. (14 April, 2020). Moscow rolls out digital tracking to enforce lockdown. Critics dub it a 'cyber Gulag'. *CNN*. https://edition.cnn.com/2020/04/14/world/moscow-cyber-tracking-qr-code-intl/index.html

170 Ball, S. (24 March, 2020). 100,000 cameras: Moscow uses facial recognition to enforce quarantine. *France24.* https://www.france24.com/en/20200324-100-000-cameras-moscow-uses-facial-recognition-to-enforce-quarantine

telefoni, kuros aktivizēta atrašanās vietas noteikšana ar GPS. Ja persona izgāja ārpus noteiktajai robežai, kurā tai jāatrodas atbilstoši pārvietošanās ierobežojumiem, viņai tika nosūtīta īsziņa un uzlikts naudas sods par pārkāpumu.[171] Kāds ASV universitātes students, kurš atradās Taivānā karantīnā, tika aizvests uz policijas iecirkni pēc tam, kad viņa telefona akumulators bija izlādējies, kamēr viņš naktī gulēja.[172]

Lai nodrošinātu obligātās mājas karantīnas ievērošanu, Honkonga ieviesa elektroniskās izsekošanas aproces.[173] Izraēlā digitālās novērošanas rīki, kurus parasti lieto pretterorisma nolūkā, tika izmantoti, lai izsekotu personas, kurām apstiprināta saslimšana ar koronavīrusu, respektīvi, noteiktu šo personu telefonu atrašanās vietu 14 dienu laikā pirms pozitīvās pārbaudes, lai noskaidrotu kontaktpersonas.[174]

Dienvidkorejā valdība izmantoja novērošanas kameru ierakstus, viedtālruņu atrašanās vietas datus un kredītkaršu ierakstus par pirkumiem, lai izsekotu pozitīvus vīrusa testu gadījumus un to kontaktus.[175]

Austrālijā[176] un ASV[177] tika ieviestas potīšu aproces, nosakot pienākumu tās uzlikt personām, kuras neievēro karantīnas vai pašizolācijas prasības.

Arī Eiropas valstīs, lai cīnītos ar pandēmiju, tika ieviestas dažādas jaunas tehnoloģijas un risinājumi, kuru izmantošanu pirms pandēmijas būtu grūti iedomāties. Piemēram, Itālija, Grieķija, Beļģija un Ungārija izmantoja dronus vai robotus, lai uzraudzītu fiziskās distancēšanās ievērošanu sabiedriskās vietās. Grieķijā un Itālijā, kā arī Vācijā Diseldorfā un Dortmundē valsts iestādes izmantoja dronus,

171 Timberg, C., Harwell, D. (19 March 2020). Government efforts to track virus through phone location data complicated by privacy concerns. *The Washington Post.* https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/

172 Stanley, J., Granick, J. S. (2020). The Limits of Location Tracking in an Epidemic. ACLU. https://www.aclu.org/wp-content/uploads/legal-documents/limits_of_location_tracking_in_an_epidemic.pdf

173 Ibid.

174 Halbfinger, D. M., Kershner, I., Bergman, R. (18 March, 2020). To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data. *The New York Times.* https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html

175 Hendry, J. (19 April, 2020). WA to electronically track COVID-19 patients who defy isolation orders. *iTnews*. https://www.itnews.com.au/news/wa-to-electronically-track-covid-19-patients-who-defy-isolation-orders-546224

176 Singer, N., Sang-Hun, C. (23 Mach, 2020). As Coronavirus Surveillance Escalates, Personal Privacy Plummets. *The New York Times*. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

177 Kallingal, M. (3 April, 2020). Ankle monitors ordered for Louisville, Kentucky residents exposed to Covid-19 who refuse to stay home. *CNN*. https://edition.cnn.com/2020/04/03/us/kentucky-coronavirus-residents-ankle-monitors-trnd/index.html

lai liktu gājējiem doties mājās un atstāt sabiedriskās vietas. Savukārt Horvātijā droni tika izmantoti, arī lai mērītu cilvēku temperatūru.[178]

Slovēnija pieņēma likumu, kas paredz, ka policija drīkst izmantot dažādas metodes, lai nodrošinātu, ka pilsoņi ievēro karantīnu un citus ierobežojošos pasākumus, un kas atļauj izmantot sejas atpazīšanu, lai apturētu un identificētu personas.[179]

Vācija ieviesa viedpulksteņa lietotni, kas vāc datus par pulsu, temperatūru un miegu, lai pārbaudītu vīrusa izraisītās slimības pazīmes. Lietotnes dati tika rādīti tiešsaistē, interaktīvā kartē, kurā iestādes var novērtēt Covid-19 sastopamības varbūtību visā valstī.[180]

Lihtenšteina, Kipra un Francija izstrādāja un ieviesa elektroniskās aproces. Lihtenšteina testēja elektronisko aproci, kas mēra ādas temperatūru, pulsu, elpošanu, asinsspiedienu. Vairāk nekā 2000 iedzīvotāju to testēja, lai noskaidrotu, vai tā var palīdzēt atklāt Covid-19 infekciju agrīnā fāzē.[181]

Savukārt Beļģijā Antverpenes ostā tika ieviestas aproces, kas izmanto *Bluetooth* tehnoloģiju, lai kontrolētu sociālās distancēšanās prasību izmantošanu darba vietā. Aproce signalizē, ja strādnieki atrodas pārāk tuvu cits citam. Turklāt Beļģijas datu aizsardzības iestāde apstiprināja, ka šādas aproces var tikt izmantotas ar nosacījumu, ka personu atrašanās vietas dati netiek vākti un glabāti, kā arī ja ir saņemta īpaša piekrišana. Brīva piekrišana gan ir visai apstrīdama, ņemot vērā, ka darba devējs un darbinieks neatrodas līdztiesīgās pozīcijās.[182]

Lai gan biometriskās valkājamās ierīces nevienā no ES valstīm nebija obligātas, tajā pašā laikā daudzie eksperimenti ar tām radīja bažas, ka turpmāk arvien biežāk varētu tikt ieviestas šāda veida ierīces un citas tehnoloģijas, kas vāc biometriskos datus un izmanto tos dažādiem mērķiem. Spilgts piemērs šādai attīstības tendencei ir Singapūra, no kuras daudzas valstis ņēma piemēru, ieviešot kontaktu izsekošanas lietotnes. Singapūra viena no pirmajām ātri ieviesa lietotni "TraceTogether", kas izmanto *Bluetooth* tehnoloģiju, nosaka un uzglabā informāciju par tuvumā esošiem telefoniem un ļauj izsekot kontaktus.[183] Lai gan

178 FRA. (2020). Coronavirus pandemic in the EU – Fundamental Rights Implications – Bulletin 2. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf

179 Kučić, L. J. (7 July, 2020). Slovenian police acquires automated tools first, legalizes them later. *Algorithm Watch*. https://algorithmwatch.org/en/slovenia-police-face-recognition/

180 Busvine, D. (7 April, 2020). Germany launches smartwatch app to monitor coronavirus spread. *Reuters.* https://www.reuters.com/article/us-health-coronavirus-germany-tech-idUSKBN21P1SS

181 Council of Europe (2020), Digital solutions to fight COVID-19.

182 Ibid.

183 Singer, Sang-Hun (23 Mach, 2020), As Coronavirus Surveillance Escalates, Personal Privacy Plummets.

lietotni lejuplādēja ceturtdaļa iedzīvotāju, t. i., 1,5 no 5,7 miljoniem, izrādījās, ka šis skaits bija pārāk mazs, lai tā varētu efektīvi palīdzēt cīnīties ar pandēmiju, savukārt obligāta tās lietošana netika noteikta, jo tā nedarbojās visās "Apple" *iOS* iekārtās. Tāpēc Singapūra nolēma izstrādāt jaunu tehnoloģiju – Covid-19 kontaktu izsekošanas valkājamo ierīci, kuru varētu izdalīt ikvienam valsts iedzīvotājam. 2020. gada septembrī Singapūra sāka šo valkājamo ierīču izdalīšanu valsts iedzīvotājiem, nosakot obligātu to lietošanu ceļotājiem, lai uzraudzītu karantīnas ievērošanu.[184]

Minētie piemēri spilgti parāda, cik ātri valstis var ieviest jaunas digitālās tehnoloģijas un risinājumus, kas ierobežo personu tiesības un brīvības. Šīs jaunās tehnoloģijas ir radījušas plašas diskusijas par to atbilstību cilvēktiesībām, īpaši tiesībām uz privātumu un datu aizsardzību, un jautājumus par to, cik lielā mērā cilvēktiesības var tikt ierobežotas ārkārtas situācijā.

Digitālo tehnoloģiju, tostarp lielo datu un mākslīgā intelekta, izmantošana vīrusa izplatības ierobežošanai un kontaktu izsekošanai rada bažas ne tikai par to ietekmi uz pamattiesībām, bet arī par šo tehnoloģiju turpmāku izmantošanu masveida novērošanas nolūkā pēc krīzes. Vēsturnieks Juvāls Noa Harari brīdina, ka mēs esam liecinieki jaunu uzraudzības sistēmu radīšanai visā pasaulē, ko veic gan valsts, gan privātie uzņēmumi. Krīze var iezīmēt nozīmīgu pavērsienu novērošanas tehnoloģiju izmantošanā, jo tā var normalizēt masveida novērošanas pasākumu izmantošanu valstīs, kuras līdz šim tos ir noraidījušas.[185] Stingra jauno tehnoloģiju izmantošanas pārraudzīšana gan pandēmijas laikā, gan pēc tās ir nepieciešama, ne tikai lai aizsargātu cilvēktiesības, bet arī lai masveida novērošanas pasākumi nekļūtu par jauno normu.

184 Mohan, M. (12 September, 2020). More than 3,500 electronic wristband devices issued to travellers serving stay-home notices: ICA. *CNA.* https://www.channelnewsasia.com/news/singapore/electronic-wristband-devices-stay-home-notice-ica-covid-19-13105390

185 Harari (2020), Yuval Noah Harari: "Every crisis is also an opportunity."

2. DAĻA

Mākslīgā intelekta novērošanas pasākumu ietekme uz cilvēktiesībām

Cilvēktiesības, demokrātija un tiesiskums ir Eiropas valstu pamatvērtības. Mākslīgais intelekts rada būtiskus izaicinājumus šīm vērtībām. Mākslīgā intelekta novērošanas pasākumi apdraud privātumu, datu aizsardzību un arī citas cilvēktiesības, uz ko lielu uzmanību ir vērsusi Eiropas Padome[186] un ES[187], kā arī citas starptautiskās organizācijas. Šie pasākumi var radīt arī plašāku negatīvu ietekmi uz demokrātiju un tiesiskumu, ko var būt grūti paredzēt un izmērīt.

Laika gaitā ir izstrādātas starptautiskas cilvēktiesību normas un to aizsardzības mehānismi, kas nosaka to, kādā veidā ir jāizturas pret ikvienu personu. ANO 1948. gada Vispārējā cilvēktiesību deklarācija[188], iespējams, ir nozīmīgākais starptautiskais cilvēktiesību dokuments, kura pamatā ir apņemšanās, ka tas, kas notika Otrā pasaules kara laikā, ir ne tikai jānosoda un jāaizliedz, bet to nekad nedrīkst atkārtot. 1966. gadā ANO pieņēma Starptautisko paktu par pilsoniskajām un politiskajām tiesībām (SPPPT)[189], kas Latvijā ir spēkā no 1992. gada 14. jūlija. Līdzās globālajām tiesību sistēmām, kāda ir ANO, cilvēktiesības ir aizsargātas arī reģionālā un nacionālā līmenī.

1949. gadā izveidotā Eiropas Padome ir izstrādājusi vienotus cilvēktiesību aizsardzības standartus, kā arī radījusi efektīvu to aizsardzības mehānismu. Viens no būtiskākajiem starptautiskajiem cilvēktiesību dokumentiem ir 1950. gada 4. novembrī Eiropas Padomes pieņemtā ECTK, kura Latvijā ir spēkā no 1997. gada. Lai nodrošinātu, ka dalībvalstis ievēro tajā noteiktās cilvēktiesības, tika izveidota ECT, kuras kompetencē ir izskatīt iedzīvotāju sūdzības un piemērot soda sankcijas

186 Sk., piemēram, Eiropas Padomes Ministru komitejas Rekomendāciju CM/Rec(2020)1 dalībvalstīm par algoritmisko sistēmu ietekmi uz cilvēktiesībām, kas pieņemta 08.04.2020.: Council of Europe (2020), Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States ..

187 Eiropas Komisija (2020), Baltā grāmata par mākslīgo intelektu; European Parliament. (2020). Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies. https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html; Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.
Vairāk par ES mākslīgā intelekta regulējumu skat. grāmatas 4.2.5. nodaļā.

188 Vispārējā cilvēktiesību deklarācija. Pieņemta 10.12.1948. (Latvijā spēkā no 22.05.1990.). https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/lat.pdf

189 Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām. Pieņemts 16.12.1966. (Latvijā spēkā no 14.07.1992.). *Latvijas Vēstnesis*, 23.04.2003., Nr. 61.

pret valsti, kas pārkāpusi viņu tiesības. Valstīm, kurām ir saistoša ECTK, ir jāievēro tajā noteiktās tiesības, kā arī ECT sniegtās atziņas par minēto tiesību interpretāciju.

Cilvēktiesību aizsardzība ieņem primāru nozīmi arī ES. Lai gan sākotnēji ES tika veidota kā ekonomiska kopiena, pakāpeniski paplašinoties tās funkcijām, arvien vairāk tika atzīta cilvēktiesību būtiskā nozīme. Līgumā par Eiropas Savienību (LES) pamattiesību ievērošanas princips ir atzīts par ES vispārējo tiesību principu, kā arī noteikts, ka ES respektē pamattiesības atbilstoši ECTK un dalībvalstu kopīgām konstitucionālām tradīcijām.[190] Būtisks solis cilvēktiesību aizsardzībā ir Hartas pieņemšana 2000. gadā. Tajā iekļautas visas ECTK noteiktās tiesības, kā arī citas tiesības un principi, kuri izriet no ES dalībvalstu kopējām konstitucionālajām tradīcijām, EST judikatūras un citiem starptautiskiem instrumentiem. Harta ir moderns tiesību akts un ietver "trešās paaudzes" pamattiesības, tostarp tiesības uz datu aizsardzību. Līdz ar Lisabonas līguma spēkā stāšanos 2009. gadā Harta kļuva par juridiski saistošu dokumentu ES iestādēm un dalībvalstīm. Izstrādājot ikvienu jaunu ES tiesību aktu, ir jāizvērtē tā ietekme un atbilstība Hartā noteiktajām pamattiesībām. ES valstīm ir pienākums ievērot Hartu, īstenojot ES tiesību aktus, ko uzrauga Eiropas Komisija, kā arī EST. Harta papildina arī valstu sistēmas, bet tās neaizstāj. Cilvēktiesības tiek nacionāli aizsargātas valstu konstitūcijās. Latvijas Republikas Satversmes (Satversme) atsevišķa nodaļa ir veltīta cilvēka pamattiesībām.

Nodaļas turpinājumā aplūkotas cilvēktiesības, kuras mākslīgā intelekta novērošanas pasākumi ietekmē visvairāk, t. i., cilvēka cieņa, privātums un datu aizsardzība, diskriminācijas aizliegums, tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu, izteiksmes brīvība, pulcēšanās un biedrošanās brīvība. Nodaļā turklāt atklāts, kā mākslīgā intelekta novērošanas pasākumi līdzās cilvēktiesību apdraudējumam var radīt arī plašāku apdraudējumu demokrātiskām vērtībām. Nodaļas nobeigumā vērsta uzmanība uz to, ka krīzes situācijās, kad valstis strauji cenšas ieviest dažādus drošības pasākumus, pienākums ievērot cilvēktiesības netiek atcelts.

2.1. Cilvēka cieņa

Cilvēka cieņas jēdziens ietver uzskatu, ka ikvienam no mums ir "iekšēja vērtība", ko nekad nedrīkst mazināt, nedrīkst apdraudēt vai apspiest citas personas, arī izmantojot mākslīgo intelektu vai citas tehnoloģijas.[191] Eiropas Datu aizsardzības

190 Līgums par Eiropas Savienību (konsolidētā versija), OV C 115/13, 09.05.2008.

191 McCrudden, C. (2008). Human Dignity and Judicial Interpretation of Human Rights. *European Journal of International Law*, 19(4), pp. 655–724. https://doi.org/10.1093/ejil/chn043

uzraudzītājs ir norādījis, ka cilvēka cieņas garantēšana varētu būt pretsvars visaptverošai novērošanai un varas asimetrijai, ar ko šobrīd saskaras indivīds. Tai ir jābūt jaunās digitālās ētikas centrā.[192]

Cilvēka cieņa ir ne tikai pamattiesība pati par sevi, bet arī visu pārējo tiesību pamats. ANO Vispārējās cilvēktiesību deklarācijas 1. pants nosaka, ka visi cilvēki piedzimst brīvi un vienlīdzīgi cieņā un tiesībās. Satversmes tiesa ir atzinusi, ka cilvēka cieņa un katra indivīda vērtība ir pamattiesību būtība.[193] No Latvijas kā neatkarīgas, demokrātiskas un tiesiskas valsts pamatnormas izriet, ka cilvēka cieņa ir valsts konstitucionāla vērtība. Cilvēka cieņa raksturo cilvēku kā augstāko demokrātiskas tiesiskas valsts vērtību. Katra indivīda vērtība ir pamattiesību būtība.[194] Tiesību zinātniece profesore Sanita Osipova norāda: "Cilvēka cieņa ir iemesls, kāpēc jāpastāv demokrātiskai tiesiskai valstij. Cieņa ir cilvēka vērtība un tiesības uz pašnoteikšanos, tā ietver brīvību un atbildību par saviem lēmumiem."[195]

Cilvēka cieņa ir gan Satversmes, gan ES tiesību pamatā. Satversmes ievadā ir norādīts, ka Latvija kā demokrātiska un tiesiska valsts balstās uz cilvēka cieņu un brīvību. Kā pamattiesība tā ir noteikta Satversmes 95. pantā, kas paredz, ka valsts aizsargā cilvēka godu un cieņu. Cilvēka cieņa kā absolūta pamattiesība ir atzīta arī ES. Tā ir noteikta LES 2. pantā un Hartas 1. pantā, kas nosaka: "Cilvēka cieņa ir neaizskarama. Tā ir jāaizsargā un jārespektē."

Cilvēka cieņa vispirms ir jāaizsargā attiecībās starp valsti un cilvēku. Vislabāk šo nepieciešamību ir izskaidrojusi S. Osipova. Viņa norāda, ka konstitucionālisms, demokrātija un tiesiska valsts, t. i., valsts, kuru mēs atzīstam par saderīgu ar mūsdienu pasauli, tika veidotas, pamatojoties uz liberālām vērtībām. Tomēr šīs radikālās izmaiņas tika panāktas tikai tāpēc, ka to prasīja jaunais uzskats – cilvēks ir saprātīgs un viņam ir tiesības uz pašnoteikšanos. Cilvēks ir vērtība, kam piešķirta neatņemama cieņa un kas ir juridiski jāaizsargā no valsts patvaļas. Tendence atbrīvot sabiedrību no iespējamiem draudiem, ierobežojot cilvēka izvēles brīvību un tiesības, spilgti izpaudās, attīstoties zinātnei, pirmkārt,

192 EDPS. (2015). Opinion 4/2015 Towards a New Digital Ethics Data, Dignity and Technology. https://edps.europa.eu/sites/default/files/publication/15-09-11_data_ethics_en.pdf

193 Satversmes tiesa ir atzinusi, ka cilvēka cieņa un katra indivīda vērtība ir pamattiesību būtība. Satversmes tiesas 2019. gada 5. marta spriedums lietā Nr. 2018-08-03; sk. arī Waldron, J. (2013). Is Dignity the Foundation of Human Rights? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2196074

194 Sk., piemēram, Satversmes tiesas 2020. gada 20. novembra spriedumu lietā 2019-33-01, 12.2. punktu un tajā citēto judikatūru.

195 Satversmes tiesa. (2020. gada 2. decembris). Satversmes tiesas priekšsēdētāja Sanita Osipova akcentē cilvēka cieņas un iecietības nozīmi pamattiesību īstenošanā. *Jurista Vārds.* https://juristavards.lv/zinas/277771-satversmes-tiesas-priekssedetaja-sanita-osipova-akcente-cilveka-cienas-un-iecietibas-nozimi-pamattiesibu-istenosana/

dabaszinātnēm. Zinātne identificēja "potenciālos draudus" sabiedrības nākotnes labklājībai, savukārt valsts ar likumiem un to piemērošanu preventīvi novērsa šos "potenciālos draudus". 20. gadsimtā mēģinājumi izmantot visjaunākos zinātniskos atklājumus sabiedrības atdzīvināšanai tika veikti daudzās valstīs, pirmkārt, identificējot "nelabvēlīgas personas" un pēc tam ierobežojot viņu tiesības un tās iznīcinot. Visiem plaši ir zināmas nacistiskajā Vācijā veiktās represijas pret noteiktu sabiedrības daļu, īpaši ebrejiem, vai komunistiskajā PSRS – pret "tautas ienaidniekiem". Tikai tiesiskas valsts un pamattiesību konsolidācija pielika punktu šausminošajiem sociālajiem eksperimentiem, kas nesamērīgi ierobežoja dažu cilvēku tiesības uz pašnoteikšanos vienā no vissvarīgākajām jomām – pašnoteikšanās pār savu ķermeni.[196]

Mūsdienās 21. gadsimtā biotehnoloģiju un informācijas tehnoloģiju straujā attīstība un apvienošanās ir radījusi daudzus jaunus jautājumus par ētiskajām un tiesiskajām robežām, līdz kādām ir pieļaujams eksperimentēt ar cilvēka ķermeni un prātu. Kā norāda ASV tiesību zinātniece Džūlija Koena (*Julie E. Cohen*), skats uz cilvēka dabu, ko pastiprina datu apstrādes algoritmi, ir gan nepiedodams, gan arī nežēlīgs.[197] Jauno tehnoloģiju, īpaši mākslīgā intelekta, attīstība, tai skaitā biometriskie masveida novērošanas pasākumi, liek no jauna pārvērtēt un noteikt skaidras sarkanās līnijas šo tehnoloģiju izmantošanai. Vislabākais veids, kā to izdarīt, ir izvērtēt šo tehnoloģiju ietekmi uz cilvēktiesībām, lai gan noteikt, kādos gadījumos tās tiek pārkāptas un nesamērīgi ierobežotas, arī nepavisam nav vienkāršs uzdevums.

Cilvēka cieņa ir būtisks elements Eiropas pieejai attiecībā uz datu apstrādi un aizsardzību. Cilvēka cieņa ir bieži ietverta nesaistošos instrumentos, kas regulē mākslīgo intelektu.[198] No cilvēka cieņas principa izriet arī cilvēka pārākuma princips, kas nozīmē arī cilvēka prioritāti pār zinātni. Atzīstot cilvēka pārākumu mākslīgā intelekta kontekstā, mākslīgā intelekta sistēmām jābūt izveidotām tā, lai tās kalpotu cilvēcei, un šo sistēmu izveidē, attīstībā un izmantošanā pilnībā jāievēro cilvēktiesības, demokrātija un tiesiskums.[199]

196 Osipova (2020), Bioethics in Correlation with the Principle of Human Dignity, pp. 121–136.

197 Cohen, J. E. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Stan. L. Rev.*, 52, pp. 1373–1438.

198 UNESCO (2021), Recommendation on the Ethics of Artificial Intelligence, point 13; OECD (2019), Recommendation of the Council on Artificial Intelligence.

199 Mantelero, A. (2020). Regulating AI within the Human Rights Framework: A Roadmapping Methodology, p. 487. In: Czech, P., Hesch, L., Lukas, K., Nowak, M., Oberleitner, G. (eds.), *European Yearbook on Human Rights.* Interesentia, pp. 477–502.

2.2. Privātums un datu aizsardzība

Mākslīgā intelekta novērošanas tehnoloģiju ieviešana un izmantošana būtiski ierobežo gan tiesības uz privāto dzīvi, gan tiesības uz personas datu aizsardzību, kas ietver arī ES datu aizsardzības regulējumu.

Tiesības uz privātumu ir starptautiski atzītas cilvēka pamattiesības, kas atrodamas galvenajos cilvēktiesību dokumentos. Tiesības uz privāto dzīvi jeb tiesības uz privātumu ir noteiktas Vispārējās cilvēktiesību deklarācijas 12. pantā, ECTK 8. pantā un Hartas 7. pantā. Tiesības uz datu aizsardzību kā patstāvīgas pamattiesības ir ietvertas Hartas 8. pantā. Lai gan šīs abas tiesības ir cieši saistītas, tās ir atšķirīgas un patstāvīgas tiesības un tiek apzīmētas arī kā "klasiskās" tiesības uz privātās dzīves aizsardzību un "modernās" tiesības uz datu aizsardzību.[200] It īpaši Eiropā šo tiesību aizsardzība tiek uzskatīta par demokrātiskas un tiesiskas valsts būtisku elementu. ES ir noteikti augsti privātuma un datu aizsardzības standarti, kas būtiski ietekmē datu aizsardzības tiesību attīstību visā pasaulē.

Tiesības uz privātās dzīves neaizskaramību noteiktas arī Satversmes 96. pantā. Satversmes tiesas praksē ir nostiprinājusies atziņa, ka Satversmes šajā pantā noteiktās tiesības uz privātās dzīves neaizskaramību ietver fiziskās personas datu aizsardzību. Konkretizējot Satversmes 96. pantā ietvertās tiesības, Satversmes tiesa ir norādījusi, ka tās aizsargā indivīda fizisko un garīgo integritāti, godu un cieņu, vārdu un identitāti, personas datus.[201]

Tiesībām uz privāto dzīvi un datu aizsardzību ir primāra nozīme, izvērtējot mākslīgā intelekta novērošanas tehnoloģijas. Grāmatas nākamajā nodaļā detalizēti analizēts, kā šīs abas pamattiesības ir piemērojamas, nosakot aizsardzības garantijas un robežas šo tehnoloģiju izmantošanai. Tāpat atklāts, kā šīs abas tiesības tiecas aizsargāt arī citas pamatvērtības, kā cilvēka cieņa un autonomija, piešķirot mums personisko sfēru, kurā varam brīvi attīstīt savu personību, domāt un veidot savu viedokli. Šīs tiesības ir būtisks priekšnoteikums arī citu cilvēktiesību īstenošanai, kuras apdraud masveida novērošanas pasākumi, piemēram, vārda un informācijas brīvības un pulcēšanās un biedrošanās brīvības īstenošanai.

Jebkura veida novērošana ir iejaukšanās tiesībās uz privātumu un tiesībās uz personas datu aizsardzību. Jau 2010. gadā profesore Helena Nisenbauma (*Helen*

200 ES Pamattiesību aģentūra, ECT, EP, EDAU (2018), Rokasgrāmata – Eiropas Savienības Pamattiesību aģentūra, Eiropas Cilvēktiesību tiesa, Eiropas Padome, Eiropas Datu aizsardzības uzraudzītājs. (2018). Rokasgrāmata par Eiropas tiesību aktiem datu aizsardzības jomā. 2018. gada izdevums. http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law

201 Sk., piemēram, Satversmes tiesas 2019. gada 6. marta spriedumu lietā Nr. 2018-11-01, 16.1. punktu; Satversmes tiesas 2016. gada 16. marta spriedumu lietā Nr. 2015-14-0103, 15.1. punktu un tajos norādītos spriedumus.

Nissenbaum) vērsa uzmanību, ka informācijas tehnoloģijas tiek uzskatītas par lieliem draudiem privātumam, jo tās ļauj visaptveroši novērot, izveidot masveida datubāzes un zibens ātrumā izplatīt informāciju visā pasaulē.[202] Ir pašsaprotami, ka mūsu privātumu apdraud nepārtrauktie tehnoloģiskie sasniegumi pēdējās desmitgadēs, tie ir padarījuši novērošanas, izsekošanas un profilēšanas paņēmienus vieglākus, lētākus un precīzākus, kā rezultātā novērošana ir ievērojami palielinājusies gan publiskajā, gan privātajā sektorā. Vēl vairāk to veicina mākslīgā intelekta un biometrisko tehnoloģiju attīstība.

Sejas atpazīšanas tehnoloģiju izmantošana ietver biometrisko datu – sejas attēlu – iegūšanu, salīdzināšanu un uzglabāšanu informācijas sistēmās identifikācijas nolūkos. Katra no šīm darbībām ir uzskatāma par iejaukšanos tiesībās uz privāto dzīvi un tiesībās uz personas datu aizsardzību. Sejas attēls ir personas dati, ko apstiprina arī EST[203] un ECT[204]. ECT ir arī atzinusi, ka sejas attēls ir viens no galvenajiem cilvēka personības atribūtiem, jo tas atklāj personas unikālās īpašības un atšķir mūs citu no cita. Tādējādi tiesības uz sejas attēla aizsardzību ir viena no būtiskākajām personības attīstības sastāvdaļām.[205]

ECTK 8. pantā ir ietverts plašs mūsu privātās dzīves aizsardzības elementu klāsts, ko var iedalīt trīs lielās kategorijās, proti:

1) personas (vispārējais) privātums;
2) personas fiziskā, psiholoģiskā vai morālā integritāte un
3) personas identitāte un autonomija.[206]

Sejas atpazīšanas tehnoloģiju ietekme uz mūsu tiesībām uz privātumu un mūsu psiholoģisko integritāti ir acīmredzama. Tajā pašā laikā arī cita veida mūsu personiskās dzīves aspektu, piemēram, uzvedības un atrašanās vietas datu, izsekošana un analīze var radīt tādu pašu ietekmi uz mūsu privātumu. Citi mākslīgā intelekta biometriskās atpazīšanas veidi, kas ietver mūsu uzvedības un emociju analizēšanu un prognozēšanu, izmantojot sejas mikroizteiksmes, balss toni, gaitu, sirdsdarbības ātrumu, vēl vairāk ietekmē mūsu psiholoģisko integritāti, dziļi iejaucas mūsu personiskajā sfērā un būtiski ierobežo spēju brīvi paust mūsu personību.

Pirmām kārtām ir svarīgi atcerēties, ka nepastāv zinātniski pierādījumi, kas apstiprina, ka personas iekšējās emocijas var tikt precīzi "nolasītas" no sejas

202 Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif: Stanford Law Books.

203 EST 2013. gada 17. oktobra spriedums lietā C-291/12 *M. Schwarz* pret *Stadt Bochum*, ECLI:EU:C:2013:670, 22., 48.–49. punkts.

204 ECT 2016. gada 12. janvāra spriedums lietā 37138/14 *Szabó and Vissy v. Hungary*, 56. punkts.

205 European Court of Human Rights (2020), Guide on Article 8 of the Convention, p. 40.

206 Ibid., p. 23.

mikroizteiksmēm, sirdsdarbības ātruma vai balss toņa. Nesenos zinātniskos pētījumos ir secināts, ka mākslīgā intelekta emociju uztveršanas sistēmas labākajā gadījumā varētu atpazīt, kā persona subjektīvi interpretē noteiktu citas personas biometrisko iezīmi. Interpretācija neatbilst tam, kā šī persona faktiski jūtas, un mākslīgais intelekts tikai apzīmē šo interpretāciju, kura ir ļoti atkarīga no konteksta un kultūras. Apgalvojumiem, ka mākslīgais intelekts varētu noteikt, piemēram, vai kāds gūs panākumus darbā vai arī ir bīstams sabiedrībai, pamatojoties uz mikroizteiksmēm vai balss toni, nav nekāda zinātniska pamata.[207] Mākslīgā intelekta sistēmu izmantošana biometriskajai identifikācijai un emociju atpazīšanai, piemēram, tiesībaizsardzībā, skolās vai darbā, ietekmē personas fizisko, psiholoģisko un morālo integritāti, kas ir personas privātās dzīves elementi.[208] Turklāt šādas tehnoloģijas aizskar arī citas pamattiesības.

2.3. Diskriminācijas aizlieguma princips

Diskriminācija ir tad, kad salīdzināmā situācijā pret vienu personu izturas mazāk labvēlīgi nekā pret citu, pamatojoties uz uztvertu vai reālu personisko pazīmi vai pazīmēm, kas ir tā sauktie "aizsargātie pamati jeb īpašības".

Hartas 21. pants aizliedz jebkāda veida diskrimināciju, tostarp diskrimināciju dzimuma, rases, ādas krāsas, etniskās vai sociālās izcelsmes, ģenētisko īpatnību, valodas, reliģijas vai pārliecības, politisko vai jebkuru citu uzskatu dēļ, diskrimināciju saistībā ar piederību pie nacionālās minoritātes, diskrimināciju īpašuma, izcelsmes, invaliditātes, vecuma vai dzimumorientācijas dēļ.

Diskriminācijas aizliegums ir noteikts ECTK 14. pantā, kas paredz, ka šajā konvencijā noteiktās tiesības un brīvības ir īstenojamas bez jebkādas diskriminācijas, tālāk uzskaitot aizsargātās pazīmes. ECTK 12. protokols nosaka, ka "jebkuru likumā paredzēto tiesību īstenošana ir nodrošināma bez jebkādas diskriminācijas", sniedzot vēl plašāku aizsargāto pamatu uzskaitījumu, kā arī tas paredz, ka nevienu nevar pakļaut diskriminācijai no publisko institūciju puses uz jebkāda pamata (1. pants).

Minēto normu formulējums izveido neizsmeļamu jeb atvērtu "aizsargāto pamatu" sarakstu, kas tādējādi var tikt attiecināts uz jaunām pazīmēm. Turklāt

207 Feldman Barrett, L., Adolphs, R., Marsella, S., et al. (2019). Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements. *Psychological Science in the Public Interest*, 20(1), pp. 1–68. https://doi.org/10.1177/1529100619832930

208 Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence – Council of Europe. Ad Hoc Committee on Artificial Intelligence (CAHAI). (2020). The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law. Report by Muller, C. https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da

Hartā atšķirībā no ECTK diskriminācijas aizliegums ir noteikts kā patstāvīgas tiesības, uz kurām var atsaukties neatkarīgi no citu tiesību īstenošanas. Minētās tiesības ir saistītas ar Hartas 20. pantā noteikto vienlīdzības principu, kas paredz, ka visas personas ir vienlīdzīgas likuma priekšā.

Saskaņā ar ECTK un ES tiesību aktiem ir iespējams pamatot atšķirīgu vai mazāk labvēlīgu attieksmi. Atšķirīga attieksme var tikt attaisnota, ja tai ir leģitīms mērķis un ja līdzekļi šī mērķa sasniegšanai ir vajadzīgi un samērīgi. Šīs robežas var atšķirties katrā konkrētajā gadījumā atkarībā no apstākļiem. Saskaņā ar ECT judikatūru atšķirīgu attieksmi, kas saistīta ar tādiem jautājumiem, kuri ir personas cieņas pamatā, piemēram, rasi vai etnisko izcelsmi un dzimumu, ir grūtāk pamatot nekā citus gadījumus.[209]

Pieņemot algoritmiskos lēmumus, kas saistīti ar datu izmantošanu, diskriminācija var rasties dažādu iemeslu dēļ, piemēram, to var radīt aizspriedumi, kas apzināti vai neapzināti ir iekļauti sejas atpazīšanas algoritma izveides, testēšanas un ieviešanas laikā, kā arī lēmumi, kādas darbības veikt, pamatojoties uz iegūtajiem rezultātiem. Mākslīgā intelekta sistēmu rezultātus būtiski ietekmē algoritmu vai programmatūras izstrādē izmantoto datu kvalitāte, kas var atspoguļot neobjektivitāti, neprecizitātes un kļūdas datu vākšanas procesā. Lai sejas atpazīšanas programmatūra būtu efektīva un precīza, tā "jāapmāca" ar lielu daudzumu sejas attēlu. Jo vairāk sejas attēlu, jo precīzākas prognozes. Turklāt precizitāti nosaka ne tikai apstrādāto sejas attēlu daudzums, bet arī to kvalitāte. Datu kvalitātei nepieciešams arī seju attēlu kopums, kas ietver dažādas cilvēku grupas. Tomēr daudzos gadījumos algoritmu izveidei tiek vairāk izmantoti baltādaino vīriešu sejas attēli, mazāk – sieviešu un citas etniskās izcelsmes personu attēli. Tāpēc sejas atpazīšanas sistēmas labi darbojas attiecībā uz baltādainiem vīriešiem, bet ievērojami sliktāk tās atpazīst melnādainos iedzīvotājus un sievietes.[210] Salīdzinot personu sejas attēlu ar attēliem datubāzē vai novērošanas sarakstā, ir lielāka kļūdas iespējamība jeb t. s. kļūdaini pozitīvie (*false positive* – angļu val.) gadījumi.

Ir veikti pētījumi, kas pierāda, ka mākslīgā intelekta algoritmi sejas atpazīšanas tehnoloģijās darbojas atšķirīgi atkarībā no personas, kura tiek identificēta,

209 FRA. (2018). Handbook on European non-discrimination law. 2018 edition, p. 93. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-non-discrimination-law-2018_en.pdf

210 Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81, pp. 77–91. http://proceedings.mlr.press/v81/buolamwini18a.html

vecuma, dzimuma vai etniskās piederības.[211] Piemēram, ASV, kur sejas atpazīšanas tehnoloģiju datubāzēs ir vairāk nekā 100 miljoni pieaugušo, sākotnējās datu kopas, kurās lielākoties ir baltādainu un vīriešu dzimuma personu attēli, ietver aizspriedumus pret tumšādainiem cilvēkiem. Sistēmai var būt lielāka kļūdas iespēja attiecībā uz citas ādas krāsas un sieviešu dzimuma personām.[212] Tādējādi šādu grupu pārstāvji var biežāk tikt diskriminēti, piemēram, daudz biežāk nepamatoti apstādināti vai aizturēti. ASV veiktajos pētījumos ir paustas bažas, ka šādas tehnoloģijas var tikt izmantotas, lai kontrolētu un izsekotu visvairāk marginalizētās kopienas un vēl vairāk atstumtu un diskriminētu noteiktas etniskās grupas, kurām jau tāpat ir pievērsta pastiprināta valsts iestāžu uzmanība.[213]

Mākslīgā intelekta uzraudzības sistēmas var radīt īpaši negatīvu ietekmi uz mazāk aizsargātām grupām, piemēram, bērniem, veciem cilvēkiem un cilvēkiem ar invaliditāti. Sejas atpazīšanas precizitāte attiecībā uz bērniem ir ievērojami zemāka.[214] Kļūdainas atbilstības risks palielinās, ja jaunībā uzņemtus sejas attēlus izmanto salīdzināšanai pēc vairāk nekā pieciem gadiem. Tas pats attiecas uz vecāku cilvēku sejas attēliem. Laiks starp attēla uzņemšanu un tā salīdzināšanu negatīvi ietekmē sejas atpazīšanas tehnoloģiju precizitāti.[215] Izvērtējot novērošanas pasākumu ieviešanu un izmantošanu, īpaši ir jāņem vērā bērnu intereses.

2.4. Bērnu tiesības

Bērnu tiesības ir noteiktas Hartas 24. pantā, kura 2. punkts uzsver, ka visās darbībās, kas attiecas uz bērnu, neatkarīgi no tā, vai tās veic valsts iestādes vai privātas iestādes, galvenokārt jāņem vērā bērna intereses. Bērna intereses kā viens no pamatprincipiem ir noteikts arī ANO Bērnu tiesību konvencijā[216], kas pieņemta

211 Sk. EDPB. (2019). Guidelines 3/2019 on processing of personal data through video devices. Version for public consultation. Adopted on 10 July 2019. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf; Wong, Q. (27 March, 2019). Why facial recognition's racial bias problem is so hard to track. *CNET.* https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack/

212 Hardesty, L. (11 February, 2018). Study finds gender and skin-type bias in commercial artificial-intelligence systems. *Massachusetts Institute of Technology.* https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

213 Sk., piemēram, Leslie (2020), Understanding bias in facial recognition technologies.

214 Michalski, D., Yiu, S. Y., & Malec, C. (2018, February). The impact of age and threshold variation on facial recognition algorithm performance using images of children. In: *2018 International Conference on Biometrics* (*ICB*), pp. 217–224, IEEE. https://doi.org/10.1109/ICB2018.2018.00041

215 FRA (2019), Facial recognition technology.

216 Bērnu tiesību konvencija. Pieņemta 20.11.1989. (Latvijā spēkā no 14.05.1992.). *Latvijas Vēstnesis*, 28.11.2014., Nr. 237.

1989. gadā un Latvijā ir spēkā no 2014. gada. Konvencija paredz, ka visās darbībās attiecībā uz bērniem neatkarīgi no tā, vai šīs darbības veic valsts iestādes vai privātas iestādes, kas nodarbojas ar sociālās labklājības jautājumiem, tiesas, administratīvās vai likumdevējas iestādes, primārajam apsvērumam jābūt bērna interesēm (3. panta 1. punkts). Valstij ir jānodrošina bērnam tāda aizsardzība un aprūpe, kas nepieciešama bērna labklājībai un attīstībai.

Bērna interesēm ir jāpievērš primārā uzmanība, attiecinot uz viņiem dažādus mākslīgā intelekta novērošanas pasākumus gan tiešā, gan netiešā veidā. ECT ir uzsvērusi, ka biometrisko datu saglabāšanai, ko veic valsts iestādes par nevainīgām nepilngadīgām personām, var būt īpaši negatīva ietekme, ņemot vērā viņu īpašo situāciju un viņu attīstības un integrācijas sabiedrībā nozīmi.[217] Īpaši būtisks jautājums ir datu vākšana par nepilngadīgajiem valstu robežu pārvaldības nolūkos. Neaizsargātās grupas, to skaitā bēgļi, saskaras ar īpašiem riskiem, jo gadījumā, ja informācija par viņiem nonāktu pie represīvajām valdībām viņu valstīs, šīs personas un viņu ģimenes tiktu pakļautas nopietnam personīgam apdraudējumam.[218]

Arvien biežāk notiek mēģinājumi izmantot sejas un citas biometriskās atpazīšanas tehnoloģijas attiecībā uz bērniem, tomēr līdz šim šos mēģinājumus ir izdevies veiksmīgi apturēt. 2019. gadā Zviedrijas datu aizsardzības iestāde piemēroja pirmo sodu par VDAR pārkāpumu par sejas atpazīšanas tehnoloģiju prettiesisku izmantošanu, lai uzraudzītu skolēnu skolas apmeklējumu.[219] Līdzīgi Francijā divas vidusskolas Nicā un Marseļā sāka izmēģināt sejas atpazīšanas tehnoloģijas, lai kontrolētu apmeklētājus pie skolu ieejas vārtiem, kuras bez maksas nodrošināja ASV tehnoloģiju uzņēmums "Cisco". Pēc nevalstisko organizāciju, skolotāju arodbiedrību un vecāku rīkotas kampaņas projekts tika apturēts un tika lūgts Francijas datu aizsardzības iestādes CNIL atzinums.[220] Iestāde atzina, ka sejas atpazīšanas tehnoloģiju izmēģināšana skolās ir prettiesiska, jo tā pārkāpj datu aizsardzības noteikumus.

Mākslīgā intelekta novērošanas tehnoloģiju ne tikai tieša, bet arī netieša attiecināšana uz bērniem ievērojami aizskar bērnu tiesības. Kā norādīts Apvienoto Nāciju Organizācijas Bērnu fonda (UNICEF) Mākslīgā intelekta politikas vadlīnijās bērniem, bērni un viņu tiesības tiek būtiski ietekmētas ne tikai tad, kad tie

217 ECT 2008. gada 4. decembra spriedums lietās 30562/04 un 30566/04 *Marper v. he United Kingdom*, 124. punkts.

218 Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement.

219 EDPB (22 August, 2019), Facial recognition in school renders Sweden's ..

220 Kayali, L. (29 October, 2019). French privacy watchdog says facial recognition trial in high schools is illegal. *POLITICO.* https://www.politico.eu/article/french-privacy-watchdog-says-facial-recognition-trial-in-high-schools-is-illegal-privacy/

tiek tiešā veidā iesaistīti mākslīgā intelekta novērošanas pasākumu īstenošanā, bet arī kad tas notiek netieši, piemēram, izmantojot novērošanas kameras un prognozējošo modelēšanu. Bērnu labklājība un pilnvērtīgas attīstības iespējas ir ierobežotas, ja augot viņu brīvību un autonomiju pastāvīgi ierobežo mākslīgā intelekta sistēmas, tostarp novērošanas sistēmas.[221] Sagaidāms, ka arvien biežāk būs sastopami mēģinājumi izmantot sejas un cita veida biometriskās atpazīšanas tehnoloģijas, to skaitā arī attiecībā uz bērniem. Tāpēc ir svarīga stipra pilsoniskā sabiedrība, kas būtu gatava aizstāvēt mazāk aizsargāto grupu un personu tiesības.

2.5. Tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu

Mākslīgā intelekta novērošanas tehnoloģijas var ierobežot arī personu tiesības uz taisnīgu tiesu un efektīvu tiesību aizsardzību. Minētās tiesības kā cilvēka pamattiesības ir nostiprinātas gan starptautiskā, gan nacionālā līmenī, sniedzot personām iespēju apstrīdēt pret viņām veiktos pasākumus, lai aizsargātu savas tiesības. Tiesības uz lietas taisnīgu izskatīšanu ir paredzētas ECTK 6. pantā. Tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu ir noteiktas arī Hartas 47. pantā, kas paredz, ka ikvienai personai, kuras tiesības un brīvības, kas garantētas ES tiesībās, tikušas pārkāptas, ir tiesības uz efektīvu tiesību aizsardzību. Satversmes 92. pants nosaka, ka ikviens var aizstāvēt savas tiesības un likumiskās intereses taisnīgā tiesā. Minētais pants tālāk paredz, ka ikviens uzskatāms par nevainīgu, iekams viņa vaina nav atzīta saskaņā ar likumu, kā arī nosaka, ka nepamatota tiesību aizskāruma gadījumā ikvienam ir tiesības uz atbilstīgu atlīdzinājumu. Mākslīgā intelekta sistēmu izmantošana tiesībaizsardzības jomā var radīt bažas par taisnīgas tiesas standartiem, īpaši nevainīguma prezumpciju, tiesībām nekavējoties tikt informētam par aizturēšanas vai apsūdzības iemeslu un būtību, tiesībām uz lietas taisnīgu izskatīšanu un tiesībām sevi aizstāvēt.[222]

Tiesības uz efektīvu tiesisko aizsardzību var tikt pārkāptas, ja valsts iestādes pret personu piemēro piespiedu pasākumus, kuru pamatā ir vienīgi sejas atpazīšanas tehnoloģiju izmantošana vai kurus ir būtiski ietekmējusi šo tehnoloģiju izmantošana, piemēram, policijas apstādināšana vai aizturēšana.[223] Sistēmas

221 UNICEF. (2020). Policy guidance on AI for children. https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

222 Council of Europe. Committee of Experts on Internet Intermediaries (MSI-NET). (2018). Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

223 FRA (2019), Facial recognition technology.

ļoti bieži kļūdās, nosakot, vai persona ir bīstama, un tas savukārt var novest pie nepamatotas aizturēšanas un apcietināšanas, kā arī to izmantošanas rezultātā var tikt apsūdzētas un pat notiesātas nevainīgas personas. Šie apsvērumi bija arī iemesls, kāpēc, piemēram, Kalifornijā šo tehnoloģiju izmantošana tika aizliegta. Proti, pastāv daudz kļūdaini pozitīvu gadījumu, t. i., kad sistēmas ieteiktā iespējamā atbilstība, pārbaudot to cilvēkam, ir izrādījusies nepareiza. Pareizi pozitīvi gadījumi, savukārt, ir sistēmas ieteiktā iespējamā atbilstība, ko operators ir atzinis par pareizu.[224]

Daudzas Apvienotās Karalistes cilvēktiesību aizsardzības organizācijas, piemēram, "Liberty" un "Big Brother Watch", ir paudušas satraukumu, kā arī ir veikti vairāki pētījumi, piemēram, Eseksas Universitātē, kas parāda, ka sejas atpazīšanas tehnoloģijas, ko izmanto policija, nepareizi atpazīst personas, un tas nozīmē, ka nevainīgi cilvēki tiek nepareizi identificēti kā potenciālie noziedznieki.[225] Londonā veiktie astoņi sejas atpazīšanas sistēmu izmēģinājumi no 2016. gada līdz 2018. gadam atklāja, ka 96 % gadījumu programmatūra kļūdaini brīdināja policiju, ka persona atbilst fotoattēlam datubāzē.[226] Kārdifas Universitātes pārskats par Dienvidvelsas policijas sejas atpazīšanas sistēmas izmēģinājumiem 2017. un 2018. gadā atklāja, ka no kopumā 2900 iespējamām atbilstībām, ko konstatēja sistēma, operatori apstiprināja 144 patiesi pozitīvos gadījumus, bet 2756 tika klasificēti kā nepareizi pozitīvi rezultāti.[227] Buenosairesā Argentīnā sejas atpazīšana pilsētas metro sistēmā 2018. gada otrajā ceturksnī izraisīja 1227 brīdinājumus, no kuriem 226 bija patiesi pozitīvi.[228]

Cik daudz no rezultātiem ir kļūdaini pozitīvi, nav precīzi nosakāms. Tomēr, pat ja sejas atpazīšanas sistēmām būtu 99 % precizitāte, kļūdaini pozitīvi rezultāti ir neizbēgami. Ja pastāv 1 % kļūdas īpatsvars, tas nozīmē, ka 100 cilvēki no 10 000 nevainīgiem pilsoņiem tiks atzīti par "meklējamiem".[229]

Viena no galvenajām problēmām ir saistīta ar to, ka tiesībaizsardzību iestāžu novērošanas pasākumu izmantošana un veids, kādā tiek iegūti un izmantoti dati,

224 Lloyd (2020), Information Technology Law, p. 5.

225 Booth, R. (3 July, 2019). Police face calls to end use of facial recognition software. *The Guardian.* https://www.theguardian.com/technology/2019/jul/03/police-face-calls-to-end-use-of-facial-recognition-software

226 Dearden, L. (7 May, 2019). Facial recognition wrongly identifies public as potential criminals 96% of time, figures reveal. *Independent*. https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html

227 Davies, B., Innes, M., Dawson, A. (2018). An evaluation of South Wales Police's use of Automated Facial Recognition. Cardiff University. https://www.statewatch.org/media/documents/news/2018/nov/uk-south-wales-police-facial-recognition-cardiff-uni-eval-11-18.pdf

228 Kayser-Bril (18 June, 2020), At least 11 police forces use face recognition ..

229 Ibid.

ir nepārredzams, kā arī nepastāv efektīvs uzraudzības un kontroles mehānisms. Datu apjoms, ko izmanto tiesībaizsardzības iestādes, var būt milzīgs. Nīderlandē policijai ir piekļuve datubāzei ar 1,3 miljoniem personu attēlu, un daudzas no šīm personām nekad nav apsūdzētas par noziedzīgu nodarījumu.[230] Francijā valsts policija var salīdzināt videonovērošanas videomateriālus ar failu, kas satur 8 miljonus personu attēlu.[231] Veids, kādā darbojas sejas atpazīšanas sistēmas un izstrādātie algoritmi, netiek kontrolēts un uzraudzīts, un šo sistēmu darbība bieži vien ir maz vai pavisam nepārredzama.

Ņemot vērā pārredzamības trūkumu, personu iespējas apstrīdēt tiesībaizsardzības iestāžu pasākumus, kas veikti, pamatojoties uz mākslīgā intelekta sistēmu rezultātiem, var būt ievērojami apgrūtinātas. Personas var nezināt, kas vāc biometriskos datus, vai pat to, ka tie tiek vākti, kā tie tiek glabāti un izmantoti utt. Tiesību uz efektīvu tiesību aizsardzību priekšnosacījums ir, ka personai ir jāapzinās, ka viņas dati ir izmantoti šādās sistēmās, piemēram, ka sejas attēls ir ietverts sejas atpazīšanas sistēmas datubāzē. Eiropas Padomes cilvēktiesību komisārs ir norādījis, ka ikvienam, kurš apgalvo, ka viņš ir publiskas iestādes, privātas organizācijas vai uzņēmuma īstenotas mākslīgā intelekta sistēmas izstrādes, ieviešanas vai izmantošanas upuris, būtu jānodrošina efektīvi tiesiskās aizsardzības līdzekļi. Valstij ir jāgarantē piekļuve efektīviem tiesiskās aizsardzības līdzekļiem tām personām, kurām ir aizdomas, ka pret viņām ir veikti pasākumi, kas pilnībā vai lielā mērā balstās uz mākslīgā intelekta sistēmas sniegto informāciju, nepārredzamā veidā un bez viņu ziņas.[232] Šīs aizsardzības garantijas detalizētāk analizētas grāmatas piektajā un septītajā nodaļā, apskatot Eiropas tiesu praksi un sniedzot politikas rekomendācijas.

Šo tehnoloģiju izmantošana var novest pie personu nepamatotas apsūdzēšanas vai tā sauktās "linča tiesas" arī tad, ja tās izmanto privātie uzņēmumi kādu labu nolūku vadīti. Piemēram, Baltkrievijas izstrādātāji paziņoja, ka strādā pie mākslīgā intelekta algoritma, kas ļauj atpazīt sejas, tādējādi ļaujot atmaskot Minskas nemieru policijas (OMON) darbiniekus, kas bijuši vardarbīgi pret mierīgiem protestētājiem, lai gan viņi ir maskās. Lai arī paziņojums par šādu iespēju izpelnījās lielu popularitāti medijos, tomēr izrādījās, ka šīs tehnoloģijas nepareizi

230 Dutch police facial recognition database includes 1.3 million people. (22 July, 2019). *DutchNews.* https://www.dutchnews.nl/news/2019/07/dutch-police-facial-recognition-database-includes-1-3-million-people/

231 Our legal action against the use of facial recognition by the French police. (21 September, 2020). La *Quadrature du Net.* https://www.laquadrature.net/en/2020/09/21/our-legal-action-against-the-use-of-facial-recognition-by-the-french-police/

232 Council of Europe Commissioner for Human Rights. (2019). Unboxing Artificial Intelligence: 10 steps to protect Human Rights. Recommendation. https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

identificēja vairākus vīriešus, kas nebija policijas darbinieki, kā arī izplatīja šo nepatieso informāciju publiski, bet vairāki policijas darbinieki, kuri, kā tika apgalvots, tika identificēti ar sejas atpazīšanas tehnoloģijām, bija jau nedēļu iepriekš identificēti.[233] Tas vēlreiz parāda, ka šo tehnoloģiju izmantošanu nevar uzskatīt par kādu burvju nūjiņu un nav pieļaujama nekritiska to ieviešana un izmantošana. Mākslīgā intelekta tehnoloģijas nav universāls brīnumlīdzeklis. Tāpēc ir svarīgi noteikt aizsardzības garantijas un izmantošanas robežas, lai novērstu to radīto negatīvo ietekmi, to skaitā novērstu politisko brīvību ierobežošanu.

2.6. Vārda un izteiksmes brīvība, pulcēšanās un biedrošanās brīvība

Tiesības uz vārda un informācijas brīvību ir noteiktas Hartas 11. pantā, kas paredz, ka ikvienai personai ir tiesības uz vārda brīvību un tās ietver uzskatu brīvību un brīvību saņemt un izplatīt informāciju vai idejas bez valsts iestāžu iejaukšanās un neatkarīgi no valstu robežām. Hartas 11. pantā noteiktās tiesības atbilst ECTK 10. pantā noteiktajām tiesībām uz izteiksmes brīvību. ECTK 10. panta 2. punkts nosaka: "Tā kā šo brīvību īstenošana ir saistīta ar pienākumiem un atbildību, tā var tikt pakļauta tādām prasībām, nosacījumiem, ierobežojumiem vai sodiem, kas paredzēti likumā un nepieciešami demokrātiskā sabiedrībā, lai aizsargātu valsts drošības, teritoriālās vienotības vai sabiedriskās drošības intereses, nepieļautu nekārtības vai noziedzīgus nodarījumus, aizsargātu veselību vai tikumību, aizsargātu citu cilvēku cieņu vai tiesības, nepieļautu konfidenciālas informācijas izpaušanu vai lai saglabātu tiesu varas autoritāti un objektivitāti."

Satversmes 100. pants paredz: "Ikvienam ir tiesības uz vārda brīvību, kas ietver tiesības brīvi iegūt, paturēt un izplatīt informāciju, paust savus uzskatus. Cenzūra ir aizliegta."

Var pastāvēt konflikts starp tiesībām uz privātumu un datu aizsardzību, no vienas puses, un vārda un izteiksmes brīvību, no otras puses. Tas ir risināts neskaitāmās Eiropas tiesvedības lietās, it īpaši saistībā ar privātas informācijas paušanu medijos. Kad informācija var apdraudēt būtiskas sabiedrības intereses, piemēram, valsts drošību, sabiedrībai var būt interese ierobežot izteiksmes brīvību, tostarp analizējot, kontrolējot un dzēšot saturu, piemēram, naida runu. Attīstot mākslīgā intelekta sistēmu spējas labāk saprast, analizēt un atklāt naida runu un pamudināšanu uz vardarbību vēlēšanu laikā, var arī palīdzēt aizsargāt

233 Aris, B. (25 September, 2020). Belarus IT specialists develope software to identify OMON officers waring masks. *bne IntelliNews.* https://www.intellinews.com/belarus-it-specialists-develop-software-to-identify-omon-officers-wearing-masks-192747/

politisko līdzdalību. Tajā pašā laikā mākslīgo intelektu var izmantot arī pretēji, lai analizētu un kontrolētu, kādu informāciju iedzīvotāji saņem, ietekmētu politiskos uzskatus un vēlēšanu rezultātus, kā to spilgti parādīja "Cambridge Analytica" skandāls. Šādā gadījumā līdzās tiesībām uz privātumu tiek aizskarta arī uzskatu brīvība.

Mākslīgā intelekta sistēmas var pārkāpt arī tiesības uz pulcēšanās un biedrošanās brīvību, kas ir noteikta Hartas 12. pantā. Minētais pants atbilst ECTK 11. pantam, kas arī paredz, ka jebkuram cilvēkam ir tiesības uz pulcēšanās un biedrošanās brīvību. Šīs tiesības var ierobežot tikai izņēmuma gadījumā. ECTK 11. panta 2. punkts paredz, ka šo tiesību izmantošanu nedrīkst pakļaut nekādiem ierobežojumiem, izņemot tiem, kas noteikti ar likumu un ir nepieciešami demokrātiskā sabiedrībā, lai aizstāvētu valsts vai sabiedrības drošības intereses, nepieļautu nekārtības vai noziegumus, aizsargātu veselību vai morāli, vai citu cilvēku tiesības un brīvības. Saskaņā ar ECTK 15. panta 1. punktu ārkārtēja sabiedriska stāvokļa gadījumā, kas apdraud nācijas dzīvi, valsts var veikt pasākumus, kas atkāpjas no ECTK ietvaros uzņemtajām saistībām tiktāl, cik to nenovēršami prasa situācijas ārkārtas raksturs, ar nosacījumu, ka šie pasākumi nav pretrunā ar citām starptautisko tiesību noteiktajām saistībām. Satversmes 103. pants nosaka, ka valsts aizsargā iepriekš pieteiktu miermīlīgu sapulču un gājienu, kā arī piketu brīvību.

Tādu novērošanas pasākumu kā sejas atpazīšanas izmantošana sabiedriskās vietās var ierobežot personas tiesības brīvi paust savus uzskatus un viedokli, kā arī pulcēšanās un biedrošanās brīvību. Šo tiesību izmantošanas nepieciešams aspekts ir grupas anonimitāte.[234] Sabiedrisku vietu novērošana ar sejas atpazīšanas tehnoloģijām var radīt atturošu efektu un likt cilvēkiem mainīt savu uzvedību. Līdzīgi ir arī gadījumā, ja valsts iestādes novēro personu darbības internetā, piemēram, ierakstus sociālajos medijos. Ja personai ir pamats baidīties, ka viņas paustais viedoklis var radīt kādas negatīvas sekas, viņa var atturēties to paust. Tādējādi tiek aizskarta personas vārda brīvība.[235]

Sabiedrības masveida novērošanas pasākumi tiešā veidā var ierobežot pulcēšanās un biedrošanās brīvību. Sejas atpazīšanas tehnoloģijas sabiedriskās vietās var negatīvi ietekmēt protestētāju vēlmi iesaistīties aktīvismā. Tās var atturēt cilvēkus apmeklēt demonstrācijas, kas ne tikai ir pretrunā ar viņu vārda brīvību, bet arī nopietni ietekmē pulcēšanās brīvību.[236] Spēju iesaistīties šādās darbībās aizsargā Harta un ECTK. Mierīgas pulcēšanās tiesības cilvēkiem dod iespēju kopīgi piedalīties savas sabiedrības veidošanā ietekmīgā, bet mierīgā veidā. Pulcēšanās brīvība aizsargā cilvēku spēju īstenot autonomiju, vienlaikus solidarizējoties ar

234 FRA (2019), Facial recognition technology.

235 UN Human Rights Council (2019), Surveillance and human rights.

236 FRA (2019), Facial recognition technology.

citiem. Sejas atpazīšanas tehnoloģiju ieviešana var radīt atturošu efektu. Personas var atturēties likumīgi īstenot pulcēšanās un biedrošanās brīvību un iesaistīties pilsoniskās līdzdalības aktivitātēs, baidoties no negatīvajām sekām, kas varētu rasties.[237] Tādējādi personas var atturēt no tikšanās ar konkrētām personām vai dalības organizācijās, sanāksmēs un demonstrācijās. Šim atturošajam efektam ir skaidra ietekme arī uz līdzdalības demokrātijas efektīvu darbību.

Vēl pirms Covid-19 vīrusa parādīšanās protestētāji Honkongā aizklāja sejas ar aizsegiem, lai aizsargātos nevis pret vīrusiem, bet lai viņas neatpazītu sejas atpazīšanas tehnoloģijas. Cilvēki, protestējot pret masveida novērošanu un viņu tiesību ierobežošanu, nogāza publiskā vietā uzstādītās videonovērošanas kameras, kas aprīkotas ar sejas atpazīšanas tehnoloģijām. Arī Serbijā Belgradā policija pret protestētājiem izmantoja sejas atpazīšanas tehnoloģijas.[238] Daudzās valstīs, piemēram, Slovēnijā, policijas iestādes izvairās publiski darīt zināmu jebkādu informāciju par šo tehnoloģiju izmantošanu, tāpat kā par citām ar to saistītām darbībām, piemēram, fotogrāfiju vākšanu un sociālo mediju kontu analīzi.[239]

Sejas atpazīšanas tehnoloģijas un citas mākslīgā intelekta biometriskās atpazīšanas tehnoloģijas rada riskus ne tikai cilvēktiesībām un drošībai, bet arī apdraudējumu demokrātijai un tiesiskumam. Tiesībām uz vārda un izteiksmes brīvību, kā arī pulcēšanās un biedrošanās brīvību ir ļoti būtiska nozīme demokrātiskā sabiedrībā. Jauno tehnoloģiju izmantošana, kas var nesamērīgi ierobežot un pārkāpt šīs brīvības, apdraud arī demokrātiskas sabiedrības pamatus.

Tendence arvien plašāk izmantot dažādus sabiedrības novērošanas pasākumus ir novērojama krīzes situācijās, kā Covid-19 pandēmijas laikā, un tas neatceļ cilvēktiesību ievērošanas prasību, kā pamatots nodaļas turpinājumā.

2.7. Pienākums ievērot cilvēktiesības krīzes situācijā

Ir labi saprotams, ka pasākumi, kas nepieciešami Covid-19 apkarošanai, neizbēgami ierobežo personu cilvēktiesības un pamatbrīvības. Ilgstoša piekļuve datiem un sistemātiska personu uzraudzība plašā mērogā, izmantojot tādas digitālās tehnoloģijas kā kontaktu izsekošanas lietotnes, ierobežo tiesības uz privātumu un datu aizsardzību.

237 Fussey, P., Murray, D. (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex, Human Rights Centre, p. 36. https://repository.essex.ac.uk/24946/

238 Serbia: Violent police crackdown against COVID-19 lockdown protesters must stop. (9 July, 2020). *Amnesty International*. https://www.amnesty.org/en/latest/news/2020/07/serbia-violent-police-crackdown-against-covid-19-lockdown-protesters-must-stop/

239 Kučić (7 July, 2020), Slovenian police acquires automated tools ..

Pastāv absolūtas cilvēktiesības, kuras nekādā gadījumā nevar ierobežot, piemēram, tiesības uz dzīvību. Tajā pašā laikā lielākā daļa cilvēktiesību, tostarp tiesības uz brīvību, tiesības uz privātumu, tiesības uz datu aizsardzību, var ierobežot, tomēr ievērojot noteiktus nosacījumus.

Saskaņā ar ECTK tādas intereses kā veselības aizsardzība un sabiedrības drošība ir pamats, lai varētu ierobežot cilvēktiesības, tomēr šādi ierobežojumi ir pieļaujami, ja tie ir "paredzēti likumā" un ir "nepieciešami demokrātiskā sabiedrībā" konkrēta mērķa sasniegšanai (8.–11. panta otrie punkti). Pēdējais nosacījums arī paredz, ka iejaukšanās tiesībās ir jābūt proporcionālai izvirzītajam leģitīmajam mērķim un ka ir piemērots vismazāk ierobežojošais līdzeklis šī mērķa sasniegšanai.[240] Minētie ierobežošanas nosacījumi atrodami arī citos cilvēktiesību dokumentos un ir atsevišķi analizēti grāmatas piektajā nodaļā.

Lai gan ārkārtas situācijās ierobežojumi var tikt piemēroti, pamatojoties uz parasto cilvēktiesību ierobežošanas kārtību veselības aizsardzības interesēs, valstīm ārkārtējā stāvokļa gadījumā var būt jāpieņem arī ārkārtas rakstura pasākumi, kuriem būtu nepieciešamas atkāpes no pienākuma ievērot noteiktas tiesības saskaņā ar starptautiskajiem cilvēktiesību dokumentiem. Šāda iespēja ir noteikta ECTK 15. pantā, un to piemēroja arī Latvija[241] un Igaunija. Šādas atkāpes tiek atzītas par pieļaujamu veidu, kā rīkoties tādās ārkārtas situācijās kā Covid-19 pandēmija, jo tās palīdz nodrošināt pārredzamību un atbildību.[242] Tomēr nav jāpieņem, ka valstis, kas piemēro šādu atkāpšanos, automātiski pārkāpj cilvēktiesības, savukārt valstis, kas izmanto parastos cilvēktiesību ierobežojumus sabiedrības veselības apsvērumu dēļ, tās nepārkāpj.

Lai gan ārkārtas situācija var attaisnot cilvēktiesības ierobežojošu pasākumu piemērošanu, tomēr tās laikā nevar atkāpties no tiesiskuma un demokrātijas principiem. Minētās atkāpes nekad nevar attaisnot darbības, kuras ir pretrunā ar galvenajām likumības, proporcionalitātes, nepieciešamības un nediskriminācijas prasībām. Kā norāda Eiropas Padome, nepieciešamības princips prasa, lai ārkārtas pasākumi sasniegtu savu mērķi, minimāli mainot parastos noteikumus. Turklāt visos ārkārtas stāvokļa laikā pieņemtajos tiesību aktos jāiekļauj arī skaidri termiņi šo ārkārtas pasākumu ilgumam, jo šāda ārkārtas stāvokļa režīma

240 European Court of Human Rights (2020), Guide on Article 8 of the Convention.

241 Sk. Līce, K., Vītola, L. E. (2020). Deklarācija starptautiskajām cilvēktiesību organizācijām par ārkārtējo situāciju Latvijā. *Jurista Vārds*, 14.04.2020., Nr. 15.

242 Sk. Spadaro, A. (2020). COVID-19: Testing the Limits of Human Rights. *European Journal of Risk Regulation*, 11(2), pp. 317–325. https://doi.org/10.1017/err.2020.27

galvenais mērķis ir ierobežot krīzes attīstību un pēc iespējas ātrāk atgriezties normālā stāvoklī.[243]

Eiropas Padomes ģenerālsekretāre Marija Peicinoviča-Buriča (*Marija Pejčinović Burić*) 2020. gada 7. aprīlī publicēja informatīvo dokumentu 46 tās dalībvalstīm. Tā mērķis ir sniegt valdībām rekomendācijas, kā risināt bezprecedenta un masveida Covid-19 sanitāro krīzi veidā, kas respektē demokrātijas pamatvērtības, tiesiskumu un cilvēktiesības.[244] Eiropas Padomes ģenerālsekretāre norāda, ka galvenais sociālais, politiskais un tiesiskais izaicinājums, ar kuru saskaras Eiropas Padomes dalībvalstis, ir to spēja efektīvi reaģēt uz Covid-19 krīzi, vienlaikus nodrošinot, ka to veiktie pasākumi nemazina patieso ilgtermiņa interesi aizsargāt Eiropas pamatvērtības – cilvēktiesības, demokrātiju un tiesiskumu.[245] Eiropas Padome izveidoja forumu, lai kolektīvi nodrošinātu, ka tiek ievēroti divi būtiski priekšnoteikumi: šie pasākumi ir proporcionāli vīrusa izplatības radītajiem draudiem un ir ierobežoti laikā. Lai gan vīruss iznīcina daudzas dzīvības un to, kas ir svarīgs, nedrīkst ļaut tam iznīcināt pamatvērtības un brīvību.

Digitālās uzraudzības tehnoloģijas var būtiski apdraudēt pamattiesības, īpaši tiesības uz privātumu un datu aizsardzību. Neskatoties uz Covid-19 krīzi, cilvēktiesības ierobežojošiem pasākumiem ir jābūt likumīgiem, nepieciešamiem un proporcionāliem pandēmijas radītajiem draudiem, un ierobežotiem laikā.

Lai ievērotu minētos nosacījumus, ieviešot jaunas uzraudzības tehnoloģijas, kā, piemēram, kontaktu izsekošanas lietotnes, ir jāizvērtē to nepieciešamība, proporcionalitāte un efektivitāte. Kaut arī šīs lietotnes tika ieviestas, lai palīdzētu aizsargāt veselību, šī aizsardzība ir pilnībā atkarīga no to efektivitātes. Noteikt, vai iejaukšanās ir proporcionāla, var nebūt vienkārši, ņemot vērā kompromisus, piemēram, starp efektivitāti un privātumu, pierādījumu trūkumu, kā arī to, ka nav skaidras izpratnes, kādas ir samērīguma prasības.[246] Tomēr, neskatoties uz šīm grūtībām, nebūtu jāizdara izvēle starp efektīvu reaģēšanu uz krīzi un pamattiesību aizsardzību.

Juvāls Noa Harari vērš uzmanību, ka patiesībā pati problēmas sakne ir prasīt, lai cilvēki izvēlas starp privātumu un veselību, jo tā ir maldīga izvēle. Mēs varam un mums vajadzētu baudīt gan privātumu, gan veselību. Mēs varam izvēlēties aizsargāt savu veselību un apturēt koronavīrusa epidēmiju, nevis ieviešot

243 Council of Europe. (2020). Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis. https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40

244 Ibid.

245 Ibid.

246 Nijsingh, N., van Bergen, A., Wild, V. (2020). Applying a Precautionary Approach to Mobile Contact Tracing for COVID-19: The Value of Reversibility. *Journal of Bioethical Inquiry*, 17, pp. 823–827. https://doi.org/10.1007/s11673-020-10004-z

totalitāras uzraudzības režīmus, bet gan dodot pilsoņiem vairāk tiesību un brīvības.[247] Arī Eiropas Datu aizsardzības uzraudzītājs Vojcehs Vjevorovskis (*Wojciech Wiewiórowski*) ir uzsvēris, ka cilvēcei nav jāapņemas panākt kompromisu starp privātumu un datu aizsardzību, no vienas puses, un sabiedrības veselību, no otras puses. Demokrātijām Covid-19 krīzes periodā ir jābūt spējīgām nodrošināt tās abas. Covid-19 uzliesmojums pārbauda mūsu sabiedrības izturību, reaģējot uz šo globālo krīzi un cenšoties ierobežot tās sekas gan īstermiņā, gan ilgtermiņā. Krīzes laikā, kā arī pēc tās pastiprināsies tādas digitālās ekonomikas tendences kā varas un informācijas nelīdzsvarotība starp nedaudziem spēcīgiem spēlētājiem un cilvēkiem, kā arī nepietiekama pārredzamība un atbildība.[248]

Strauji pieaugošā tendence, kas īpaši ir pastiprinājusies Covid-19 krīzes laikā, kad mākslīgā intelekta un cita veida novērošanas tehnoloģijas tiek izmantotas pretēji demokrātiskām pamatvērtībām, apliecina nepieciešamību pēc iespējas ātrāk pieņemt skaidru regulējumu, kas paredzētu atbildību, uzliktu pienākumu valsts iestādēm būt atklātām un informēt sabiedrību par to izmantošanu, kā arī noteiktu šo tehnoloģiju izmantošanas sarkanās līnijas. Lai to panāktu, ir būtiski mēģināt saprast, kā esošais regulējums un garantijas, īpaši privātuma un datu aizsardzības regulējums, ir piemērojamas šīm jaunajām tehnoloģijām, kā tās būtu jāattīsta un jāpapildina. Šim jautājumam veltīta nākamā nodaļa.

247 Harari (20 March, 2020), Yuval Noah Harari: the world after coronavirus.

248 Wiewiórowski, W. (30 April, 2020). Carrying the torch in times of darkness. *EDPS.* https://edps.europa.eu/press-publications/press-news/blog/carrying-torch-times-darkness_en

3. DAĻA

Privātuma nozīme

Privātums un datu aizsardzība vairs nav tikai juridiskos tekstos lietoti termini. Tie ir kļuvuši populāri un bieži dzirdami vārdi jaunākajos ziņu sižetu un žurnālu virsrakstos, īpaši – apskatot tehnoloģiju uzņēmumu liela apjoma datu iegūšanas un izmantošanas bieži vien prettiesisko un patvaļīgo praksi, kā arī jaunu aizskarošu tehnoloģiju ieviešanu gan valsts, gan privātajā sektorā. Tajā pašā laikā rodas jautājumi: kādu labumu sabiedrībai un ikvienam no mums sniedz privātums un kāpēc tas ir nepieciešams. Lai gan tiesības uz privātumu ir ietvertas daudzos cilvēktiesību dokumentos, neviens no tiem nepaskaidro, kas ir privātums un kāpēc tas ir jāaizsargā. Šajā nodaļā apskatītas dažādas teorijas, kas skaidro privātuma nozīmi un tā aizsardzības pamatojumu, un ir atklāts, ka privātumam gan kā cilvēka pamattiesībai, gan kā ētiskai un sociālai vērtībai ir izšķiroša nozīme, lai ierobežotu mākslīgā intelekta masveida novērošanas praksi.

Privātuma definēšana nav vienkāršs uzdevums, jo par šī jēdziena nozīmi, vērtību un darbības jomu domas dalās. Tiesību zinātniece Liliana Edvardsa (*Lilian Edwards*) norāda, ka privātums ir īpaši sarežģīta vērtība un tam ir grūti izstrādāt regulējumu, galvenokārt tāpēc, ka ir maz vienprātības par to, kas tas patiesībā ir.[249] Turklāt daudzi zinātnieki ir arī kritizējuši privātumu. Daži no kritiķiem norāda, ka privātums nav uzskatāms par atsevišķām tiesībām. Filozofe Džūdita Džārvisa Tomsone (*Judith Jarvis Thomson*) 1975. gadā rakstīja, ka vispārsteidzošākais saistībā ar tiesībām uz privāto dzīvi ir tas, ka, šķiet, nevienam nav skaidra priekšstata, kas tas ir, turklāt visas dažādās aizsardzības, uz kurām, mūsuprāt, tiesības uz privātumu attiecas, mēs jau esam iekļāvuši citās tiesībās.[250]

Citi kritiķi, savukārt, atzīst, ka privātums ir ļoti subjektīva vērtība, nevis objektīvs jēdziens, kas ir vienlīdz svarīgs visiem cilvēkiem. Kamēr vieniem tādas mūsdienu privātumu ierobežošanas prakses kā sejas atpazīšanas sistēmas var likties pieņemamas, citi stingri iebilst pret šādu biometrisko datu izmantošanu. Ja privātumu uzskata par individuālām interesēm, to ir grūti līdzsvarot ar tādām sociālajām interesēm, kā, piemēram, drošība, sabiedrības drošība, inovāciju un

249 Edwards, L. (ed.). (2019). *Law, Policy, and the Internet*. Oxford, UK; Portland, Orego: Hart Publishing, p. 51.

250 Sk. Thomson, J. J. (1975). The Right to Privacy. Philosophy and Public Affairs, 4(4), pp. 295–314.

ekonomikas izaugsme.[251] Tomēr alternatīvu pieeju, kas paredz objektīvi novērtēt, kādu kaitējumu – ekonomisku, emocionālu vai cieņas – rada privātuma aizsardzības pasākumu trūkums, ir arī ļoti grūti īstenot.[252]

Lai gan ir daudz kritisku uzskatu, tiesību zinātnieki lielākoties tomēr aizstāv privātumu kā nozīmīgu jēdzienu.

3.1. Tiesības palikt vienam

Pirmie privātuma definēšanas mēģinājumi notika jau 19. gadsimtā, kad divi ASV juristi Semjuels Vorens (*Samuel D. Warren*) un Luijs Brendaiss (*Louis D. Brandeis*) savā slavenajā esejā "Tiesības uz privātumu" (*The Right to Privacy* – angļu val.) apzīmēja privātumu kā "tiesības palikt vienam", ko var iztulkot arī kā "tiesības uz likšanu mierā" (*the right to be let alone* – angļu val.).[253] Šis 1890. gadā "Harvard Law Review" publicētais darbs bieži tiek uzskatīts par visietekmīgāko tiesību pārskata rakstu, kāds jebkad ir publicēts.[254]

Autori darbā vērsa uzmanību, ka politiskās, sociālās un ekonomiskās pārmaiņas nozīmē jaunu tiesību atzīšanu un paplašina esošo kopējo tiesību aizsardzību, lai apmierinātu sabiedrības prasības.[255] Jaunākie izgudrojumi un uzņēmējdarbības metodes liecina par nākamo soli, kas jāsper personas aizsardzībai un indivīda tiesību palikt vienam nodrošināšanai. Vispārējās tiesības (*common law* – angļu val.) parasti nodrošina katram cilvēkam tiesības izlemt, cik daudz viņa domas, izjūtas un emocijas atklāt citiem.[256] Spēkā esošās tiesības nosaka principus, kurus var izmantot, lai aizsargātu indivīda privātumu no pārāk uzmācīgas preses, fotoaparātu vai citu modernu ierīču, kas ieraksta attēlus vai skaņas, īpašniekiem.[257] Vispārējās tiesības ir attīstījušās no fiziskas personas un ķermeņa aizsardzības līdz indivīda domu, emociju un sajūtu aizsardzībai, kas tagad prasa juridisku atzīšanu. Šīs tiesības jau pastāv Lielbritānijā lietās par īpašuma tiesībām, kas ļauj, piemēram, literāru darbu autoriem absolūti kontrolēt to publicēšanu.[258] Tomēr šo

251 Edwards (2019), *Law, Policy, and the Internet*, p. 51; sk. arī Bennett, C. J., Raab, C. D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. (2nd and updated ed.) Cambridge, Mass: MIT Press, p. 8.

252 Edwards (2019), *Law, Policy, and the Internet*, p. 53.

253 Warren, S., Brandais, L. D. (1890). The right to privacy. *Harward Law Review*, 4, pp. 193–220. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

254 Edwards (2019), *Law, Policy, and the Internet*, p. 59.

255 Warren, Brandais (1890), The right to privacy, p. 193.

256 Ibid., p. 198.

257 Ibid., p. 206.

258 Ibid., pp. 199–200.

tiesību pamatā nav īpašuma aizsardzība, bet gan tiesības uz privātumu, tās ir daļa no vispārīgākām personas imunitātes tiesībām – tiesībām uz "personas neaizskaramību".[259] Šīs tiesības nav atkarīgas ne no domu un emociju izteikšanas veida (piemēram, vārdi, zīmes, glezniecība, skulptūra, mūzika), ne no tā, vai tās tiek izteiktas literāros vai mākslinieciskos skaņdarbos vai arī ikdienā.[260] Vienlīdz aizsargājams ir, piemēram, dienasgrāmatas ieraksts un dzejolis. Domas, emocijas un izjūtas ir aizsargājamas vienādi neatkarīgi no tā, vai tās ir izpaustas rakstiski, uzvedībā, sarunā, attieksmē vai sejas izteiksmē.[261] Jebkurā gadījumā indivīdam ir tiesības izlemt, vai tās tiek atklātas sabiedrībai.[262]

Lai gan eseja ir sarakstīta vairāk nekā pirms gadsimta, tajā paustie argumenti mūsdienās šķiet vēl aktuālāki nekā tajā laikā. Vai personai ir jābūt pašai tiesīgai noteikt, cik lielā mērā tiek atklātas domas, emocijas un sajūtas, ir viens no galvenajiem jautājumiem, kas pamato nepieciešamību noteikt jauno biometrisko novērošanas tehnoloģiju, kā sejas atpazīšanas un emociju uztveršanas tehnoloģijas, izmantošanas robežas.

S. Vorena un L. Brendaisa eseja aizsāka privātuma tiesisku atzīšanu ASV, un pakāpeniski tika paplašināta tiesību uz privātumu aizsardzība. Lai gan ASV Konstitūcijā termins "tiesības uz privātumu" neparādās, ASV Augstākā tiesa tās ir atzinusi par konstitucionālām tiesībām. 1928. gadā L. Brendaiss bija kļuvis par Augstākās tiesas tiesnesi, un viņš paziņoja, ka ASV Konstitūcijā ir piešķirtas "tiesības palikt vienam", kas paredz, ka valdības nepamatota iejaukšanās indivīda privātajā dzīvē neatkarīgi no izmantotajiem līdzekļiem jāuzskata par ASV Konstitūcijas ceturtā labojuma pārkāpumu.[263] Konstitūcijas ceturtais labojums regulē valdības novērošanu un novērš patvaļīgu privātuma aizskaršanu.[264] Tomēr, neskatoties uz privātuma tiesību atzīšanu, ASV ir izstrādājusi ierobežotu privātuma aizsardzības sistēmu, un tai trūkst tiesību uz privātumu visaptveroša federāla regulējuma. Atšķirībā no Eiropas Savienības ASV vairāk paļaujas uz industrijas pašregulāciju un parasti atbalsta pozīciju, ka bizness un valdība var brīvi piekļūt datiem, lai garantētu ekonomikas izaugsmi vai valsts drošību.[265]

259 Warren, Brandais (1890), The right to privacy, p. 207.

260 Ibid., pp. 198, 207.

261 Ibid., p. 206.

262 Ibid., pp. 198–199.

263 Monti, A., Wacks, R. (2019). *Protecting Personal Information: The Right to Privacy Reconsidered*. Oxford: Hart Publishing, p. 11. https://doi.org/10.5040/9781509924882

264 Sk. Tokson, M. (2020). The Emerging Principles of Fourth Amendment Privacy. *The George Washington Law Review*, 88(1). https://www.gwlr.org/wp-content/uploads/2020/05/88-Geo.-Wash.-L.-Rev.-1.pdf

265 DeCew, J. (2018). Privacy. In: Zalta, E. N. (ed.). *The Stanford Encyclopedia of Philosophy.* https://plato.stanford.edu/archives/spr2018/entries/privacy/

Privātums tā tradicionālajā aspektā ir skatīts kā personas interese netikt pakļautai nevēlamai uzmanībai no valsts vai trešās personas puses.[266] Tāpat Vorens un Brendaiss ielika pamatu izpratnei, ka privātums ietver arī tiesības kontrolēt informāciju par sevi.[267]

3.2. Tiesības kontrolēt informāciju par sevi

Mūsdienās privātumu primāri aplūko kā tiesības kontrolēt informāciju par sevi. Privātums tiek pamatots kā spēja personai pašai noteikt, kad, kā un cik daudz informācijas tiek atklāts citiem.[268] Uzskats, ka personai ir jāatdod kontrole pār saviem datiem, ir pamatā arī ES datu aizsardzības regulējumam. Saskaņā ar šo uzskatu, mēs vienmēr varam izvēlēties, vai dalīties ar savu personisko informāciju un vai atklāt savu iekšējo būtību citiem. Tomēr šī definīcija nepaskaidro, ko var uzskatīt par personisku informāciju, kuru indivīdam ir tiesības kontrolēt.[269] Ir daudz diskusiju par to, kāda ir šī informācija un kādu iemeslu dēļ tā ir jāaizsargā.

Tiklīdz mēs esam brīvprātīgi dalījušies ar savu personisko informāciju, zaudējam kontroli pār tās turpmāko izmantošanu, bet tas nenozīmē, ka informāciju, ko atklājam konkrētam mērķim, var brīvi izmantot, jo mums joprojām saglabājas zināma kontrole pār to. Tomēr šī teorija neatklāj privātuma aizsardzības nepieciešamības pamatojumu. Vēl jo vairāk, vēsture rāda, ka mūsu tiesības kontrolēt personisko informāciju var viegli atņemt gan valdība, gan privātie uzņēmumi. Turklāt līdz ar informācijas sabiedrības attīstību un lielo tehnoloģiju uzņēmumu varas milzīgo pieaugumu šī kontrole mūsdienās ir kļuvusi par ilūziju.

Daudzi zinātnieki joprojām atbalsta šo šauro viedokli, ierosinot tiesības uz privātumu definēt kā tiesības kontrolēt personisko informāciju un nodrošināt garantijas, lai to aizsargātu.[270] Tomēr tādējādi tiek būtiski sašaurināta to nozīme.

Lai arī izpratne par privātumu kā tiesībām "palikt vienam" ir pievilcīga savā vienkāršībā, tā rada jaunu jautājumu: kāpēc persona vēlas, lai to liek mierā, vai kāpēc tai ir nepieciešams palikt vienai? Līdzīgs jautājums rodas arī attiecībā uz šo teoriju, proti: kāpēc mums ir nepieciešams kontrolēt informāciju par sevi?

266 Van Dijk, et al. (eds.). (2018). *Theory and Practice of the European Convention on Human Rights*. 5th ed. Cambridge; Antwerp; Portland: Intersentia, p. 670.

267 DeCew (2018), Privacy.

268 Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum; Hoven, J. van den, et al. (2014, 2019 ed.). Privacy and Information Technology. In: Zalta, E. N. (ed.), *The Stanford Encyclopedia of Philosophy*. https://plato.stanford.edu/archives/sum2020/entries/it-privacy/

269 Solove, D. J. (2009). *Understanding Privacy*. Cambridge, Massachusetts London, England: Harvard University Press, p. 82.

270 Monti, Wacks (2019), *Protecting Personal Information*, p. 128.

3.3. Cilvēka cieņas un autonomijas būtisks aspekts

Privātuma vērtību galvenokārt pamato divi viedokļi. No vienas puses, tiek uzskatīts, ka privātums ir patstāvīga vērtība un neatņemamas tiesības, kas raksturīgas indivīda kā "cilvēka" pastāvēšanai. Šajā ziņā privātums ir saistīts ar cilvēka cieņu, autonomiju un personību, un tiek uzskatīts, ka privātuma aizskārumi pārkāpj šīs vērtības. No otras puses, privātuma lietderība izpaužas kā dažādu labumu, ko gūst gan indivīdi, gan sabiedrība, veicināšana, kuri rodas no privātuma aizsardzības vai kurus samazina privātuma pārkāpumi, piemēram, valsts iestāžu varas prettiesiska izmantošana.[271]

Pirmo viedokli aizstāv vairāki teorētiķi, uzskatot privātumu par būtisku cilvēka cieņas un autonomijas aspektu.[272] Profesors un datoru drošības speciālists Brūss Šneiers (*Bruce Schneier*) uzsver, ka privātums ir cilvēka pamattiesība, kas raksturīga ikviena cilvēka cieņai.[273]

H. Nisenbauma uzskata, ka attiecības starp privātumu un autonomiju digitālajā kontekstā izpaužas vairākos veidos. Privātums nodrošina autonomiju attiecībā uz mūsu personisko informāciju, un tas arī rada vidi, kurā mēs varam izmantot savu autonomiju, justies brīvi domās un darbībā, kas nebūtu iespējams pastāvīga novērošanas riska apstākļos. Turklāt privātums ļauj mums izdarīt brīvas izvēles un rīkoties brīvi, aizsargājot pret manipulācijām ar mūsu izvēli un rīcību.[274]

Eiropas Savienības Tiesas tiesnese, Latvijas tiesību zinātniece profesore Ineta Ziemele vērš uzmanību, ka mūsu liberālā pasaules redzējuma centrā ir viena pamatvērtība – katra cilvēka cieņa. Šajā ziņā privātums ir būtisks cilvēka cieņas elements. Tā ir nepieciešama cilvēka pašnoteikšanās daļa, kas ir viena no īpašībām, kas virza cilvēka evolūciju. Tādējādi privātums, piešķirot mums mūsu privāto telpu, kā arī ļaujot izpaust mūsu izvēles brīvību un brīvo gribu, ir cieši saistīts ar cilvēka cieņu.[275]

271 Sk. Tzanou, M. (2019). *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*. Oxford: Hart Publishing, p. 8.

272 Bernal, P. (2015). *Internet Privacy Rights Rights to Protect Autonomy*. Cambridge: Cambridge University Press, p. 33. http://dx.doi.org/10.1017/CBO9781107337428

273 Schneier (2016), *Data and Goliath* .., p. 148; sk. arī Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. *Philosophy & Technology*, 29(4), pp. 307–312. https://doi.org/10.1007/s13347-016-0220-8

274 Sk. Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79(119). https://core.ac.uk/download/pdf/267979739.pdf; Nissenbaum (2010), *Privacy in context: Technology, Policy and Integrity of Social life.*

275 Ziemele, I. (31 January, 2020). Opening of the Judicial Year Seminar. The European Convention on Human Rights: Living Instrument at 70 – Science and Technology. https://echr.coe.int/Documents/Speech_20200131_Ziemele_JY_ENG.pdf

Privātums dod mums personisko sfēru, kurā varam brīvi attīstīt savu personību, domāt un veidot savu viedokli. Pasaulē, kur tiek aizsargāts privātums, kur maz pazīstam cits citu, cilvēki var brīvi rīkoties, kā viņi vēlas, jo pastāv mazs sociālais spiediens, kas viņus varētu ierobežot. Privātums atbalsta daudzveidību. Tur, kur cilvēki ir aizsargājuši privāto sfēru, viņiem ir brīvība atšķirties no sabiedrības vairākuma uzskatiem un ideāliem. Jo vairāk mēs cits par citu zinām, jo vairāk mēs varam uzspiest sociālās normas. Tādējādi privātuma vērtību nosaka arī sabiedrības atvērtība. Neiecietīgā sabiedrībā privātums ir ļoti vērtīgs, it īpaši, ja jūs kaut kādā veidā atkāpjaties no vispārpieņemtajām normām.[276]

Viens no izplatītākajiem nepareizajiem uzskatiem par privātumu ir, ka tas palīdz tikai likumpārkāpējiem vai kādam, kam ir kaut kas slēpjams.[277] Tomēr nav nekas slikts dziedāt dušā vai stāstīt intīmus noslēpumus tikai labākajam draugam, bet ne vecākiem vai kolēģiem. Mēs parādām dažādus savus aspektus dažādiem cilvēkiem – draugiem, bērniem, vecākiem – un dažādās dzīves lomās – profesionālajā dzīvē un brīvajā laikā, mēs neatklājam visu savu dzīvi sociālo mediju ziņās.

Mums jāapzinās, ka autonomija un brīva griba ir būtisks nosacījums morālajai rīcības brīvībai.[278] Mēs neesam atbildīgi par sekām, kuras nevarējām izvēlēties vai novērst. J. N. Harari vērš uzmanību, ka būtu naivi domāt, ka neviens nevar veiksmīgi paredzēt un manipulēt ar personas izvēli, jo šī izvēle atspoguļo personas brīvo gribu. Viņš brīdina, ka biotehnoloģijas un informācijas tehnoloģiju revolūcija var ļaut lielo datu algoritmiem daudz labāk par pašu personu izprast tās jūtas un pat domas. Tiklīdz lielākajām interneta kompānijām izdosies dziļāk izprast, kā cilvēki pieņem lēmumus, persona tiks pakļauta precīzām vadītām manipulācijām un propagandai. "Facebook" un "Cambridge Analytica" skandāls bija tikai pirmais brīdinājums.[279]

Iepriekš jau tika norādīts, ka viens no galvenajiem mākslīgā intelekta apdraudējumiem ir algoritmiskā manipulācija, kas rada draudus mūsu autonomijai.[280] Mašīnmācīšanās rīkiem ir arvien lielāka spēja ne tikai prognozēt mūsu izvēles, bet arī ietekmēt emocijas un domas un mainīt paredzamo rīcību, dažkārt pat ietekmējot zemapziņu. Šos rīkus var izmantot, lai manipulētu un kontrolētu ne

276 Donath, J. (2020). Privacy and Public Space. In: *The Social Machine. Design for living online*. https://covid-19.mitpress.mit.edu/pub/8icuynaf

277 Schneier (2016), *Data and Goliath* .., p. 147.

278 Weissman, D. (2018). Autonomy and Free Will: Autonomy and Free Will. *Metaphilosophy*, 49(5), pp. 609–645. https://doi.org/10.1111/meta.12333

279 Harari, Y. N. (14 September, 2018). Yuval Noah Harari: the myth of freedom. *The Guardian.* https://www.theguardian.com/books/2018/sep/14/yuval-noah-harari-the-new-threat-to-liberal-democracy

280 Susser, D., Roessler, B., Nissenbaum, H. (2019). Technology, Autonomy, and Manipulation. *Internet Policy Review,* 8(2). https://doi.org/10.14763/2019.2.1410

tikai ekonomisko izvēli, bet arī sociālo un politisko uzvedību.[281] Vadīšana vai kontrolēšana ārpus mūsu apzinātās izpratnes pārkāpj mūsu autonomiju, spēju saprast un patstāvīgi veidot savu dzīvi.[282]

Oksfordas Interneta institūta profesors Lučāno Florīdi (*Luciano Floridi*) uzskata, ka cilvēka cieņa tiešā veidā pamato tiesību uz privātumu aizsardzību. Cilvēka cieņa ir pamatjēdziens, kas nodrošina ietvaru, kurā piemērojamas un interpretējamas tiesības uz privātumu, kā arī datu aizsardzības noteikumi. Viņš tēlaini salīdzina cilvēkus ar ceļotājiem, kuru dzīvi veido dažāda veida informācija. Cilvēki ir kā ceļotāji, kas atkarīgi no daudziem mūsu dzīves vadītājiem: citiem cilvēkiem, fiziskās pasaules, sabiedrības, kultūras, pasaules, kuru mēs radām, ne tikai tās, kurā mēs sevi atrodam. Šajā ceļojumā mums vajadzētu baudīt tiesības uz aizsardzību un viesmīlību. Katrs no mums ir skaista, bet trausla un ļoti maināma vienība. Mūsu cieņa balstās uz to, ka spējam būt kapteiņi mūsu pašu ceļojumos un saglabāt savu identitāti un izvēles iespējas. Jebkura tehnoloģija vai politika, kas tiecas novērst un mazināt šādu atvērtību, riskē mūs dehumanizēt. Tādējādi cilvēka cieņa nodrošina pamatu tiesībām uz privātumu un individuālu kontroli pār informāciju, kas veido un ietekmē cilvēka dzīvi.[283]

3.4. Aizsardzība pret varas ļaunprātīgu izmantošanu

No cita skatpunkta, privātumam ir būtiska nozīme, lai aizsargātu pret varas ļaunprātīgu izmantošanu un nodrošinātu demokrātijas principu ievērošanu. Privātums ir kā "aizsargs pret valdības apspiešanu un totalitārajiem režīmiem", un tam ir vērtība, jo tas ierobežo apspiešanas spēkus un despotiskus režīmus.[284] Privātuma trūkums tiek pielīdzināts valsts uzraudzībai un uzskatīts par totalitāras valsts pazīmi.[285]

Senajā Grieķijā un Romā privātums tika uzskatīts par "aizdomīgu" un "sociāli kaitīgu", jo tas aizstāv norobežošanos no sabiedrības. Privātums nozīmēja "stāvokli, kad kaut kas tiek atņemts".[286] Saskaņā ar kristietības filozofiju labiem cilvēkiem nav nekā slēpjama ne no Dieva, ne no citiem. Grēku izsūdzēšana

281 Council of Europe (2019). Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes. https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4b

282 Susser, Roessler, Nissenbaum (2019), Technology, Autonomy, and Manipulation.

283 Sk. Floridi (2016), On Human Dignity as a Foundation for the Right to Privacy, pp. 307–312.

284 Sk. Tzanou (2019), *The Fundamental Right to Data Protection*, p. 8.

285 Lloyd (2020), Information Technology Law, p. 3.

286 Tzanou (2019). *The Fundamental Right to Data Protection*, p. 9.

(faktiski – informācijas izpaušana) ir veids, kā grēki tiek atlaisti, lai Dievs piedotu izdarīto. Šo teoriju vēlāk pārņēma tādi republikāņu filozofi kā Žans Žaks Ruso (*Jan Jacques Rouseau*), kuri privātas problēmas uzskatīja par draudiem valdības darbībām un par valsts beigām.[287]

Informācijas privātums kā jēdziens sakņojas kopējās bailēs par individuālo privātumu, ko rada atmiņas par nacistu lietu glabāšanu Otrā pasaules kara un pēckara staļinisma laikā. Rietumu valstīs, kad 20. gadsimta 40. un 50. gados pasaule tika atjaunota, pastāvēja lielas bailes no totālas uzraudzības "lielā brāļa" valsts, ko varēja novērot Vācijā un totalitārajā padomju blokā un kuru savos darbos iemūžināja Džordžs Orvels.[288] Šīs bailes Eiropā vēl joprojām ir spilgtā atmiņā. Tādējādi vēsturiski privātums tiek uzskatīts par brīvības elementu, kas dod tiesības būt brīvam no valsts iejaukšanās.[289] Tas ietver vispārēju iejaukšanās aizliegumu un aizsargā pret varas prettiesisku vai pārmērīgu izmantošanu. Nepieciešamība pēc šāda veida aizsardzības bija pamats, lai pēc Otrā pasaules kara tiesības uz privāto dzīvi nostiprinātu galvenajos cilvēktiesību līgumos.

3.5. Tiesības uz privātumu cilvēktiesību dokumentos un to nozīme citu tiesību aizsardzībā

Privātums ir atzīts par universālām cilvēktiesībām. Tās ir noteiktas galvenajos starptautisko cilvēktiesību dokumentos. ANO Ģenerālā asambleja pieņēma un pasludināja Vispārējo cilvēktiesību deklarāciju, kuras 12. pants nosaka: "Nedrīkst patvaļīgi pārkāpt neviena cilvēka privātās dzīves, ģimenes, mājokļa un korespondences neaizskaramību, ne arī apdraudēt viņa godu un reputāciju. Katram cilvēkam ir tiesības uz likuma aizsardzību pret šādiem pārkāpumiem vai apdraudējumiem."

Līdzīgi SPPPT 17. panta pirmā daļa nosaka: "Nedrīkst patvarīgi vai nelikumīgi iejaukties neviena privātajā vai ģimenes dzīvē, apdraudēt mājas neaizskaramību vai korespondences noslēpumu vai nelikumīgi uzbrukt viņa godam un reputācijai." Minētā panta otrā daļa tālāk paredz: "Ikvienam ir tiesības uz likuma aizsardzību pret šādu iejaukšanos vai šādiem apdraudējumiem."

Eiropas tiesību sistēmā tiesības uz privāto dzīvi ir noteiktas ECTK 8. pantā, kura 1. punkts nosaka: "Ikvienam ir tiesības uz savas privātās un ģimenes dzīves, dzīvokļa un korespondences neaizskaramību." Minētā panta otrā daļa paredz

287 Tzanou (2019). *The Fundamental Right to Data Protection*, p. 9.

288 Edwards (2019), *Law, Policy, and the Internet*, p. 59.

289 Rainey, B., McCormick, P., Ovey, C. (2021). *Jacobs, White, and Ovey: The European Convention on Human Rights*. Oxford University Press, p. 411.

aizliegumu valsts institūcijām traucēt šo tiesību realizāciju, izņemot likumā noteiktos gadījumos un ja tas ir nepieciešami demokrātiskā sabiedrībā, lai īstenotu būtiskākas sabiedrības intereses vai lai aizstāvētu citu personu tiesības un brīvības. Gandrīz katra pasaules valsts kaut kādā veidā atzīst privātumu, vai tas būtu konstitūcijā vai citā regulējumā.

Privātums ir būtisks priekšnoteikums arī citu pamattiesību un pamatbrīvību īstenošanai, piemēram, vārda un izteiksmes brīvības, mierīgas pulcēšanās un biedrošanās brīvības un reliģijas brīvības īstenošanai.[290]

Valsts iestāžu, kā arī uzņēmumu uzraudzības rezultātā cilvēkiem pieejamā privātā telpa samazinās, un tas rada atturošu ietekmi uz cilvēku spēju un vēlmi brīvi izteikties un darboties, tostarp pilsoniskajā jomā, kas ir ļoti būtiska demokrātijai.[291]

Mākslīgā intelekta sistēmas ir veidotas un "barotas" ar datiem. Ja viss, ko kāds saka un dara, tiek izsekots un uzraudzīts, tas atstāj atturošu ietekmi uz to, ko cilvēks saka brīvi, kur tas var brīvi doties un ar ko brīvi tikties. Ja esat disidents, tas ietekmēs jūsu spēju kritizēt valdību. Tā ir autoritāras valdības masveida novērošanas būtība – ka cilvēki paši sevi regulē un cenzē.[292]

Privātuma zaudēšana tieši apdraud pulcēšanās, biedrošanās un izteiksmes brīvību. To, cik daudz privātuma zudums var ietekmēt šo pamattiesību īstenošanu, spilgti parāda privātumu aizskarošu tehnoloģiju (kā sejas atpazīšanas tehnoloģijas un telefonu atrašanās vietas izsekošana) izmantošana, lai identificētu protesta akciju dalībniekus, ko varēja novērot, piemēram, Honkongā un Indijā protestu laikā.[293]

Arī Eiropas demokrātiskās valstīs novērošanas tehnoloģiju izmantošana sabiedriskās vietās var ietekmēt personas uzskatu un vārda brīvību, tostarp tāpēc, ka šīs brīvības izmantošanas obligātais aspekts ir grupas anonimitāte. Apziņa, ka, lai uzraudzītu sabiedriskas vietas, tiek izmantotas sejas atpazīšanas tehnoloģijas, var likt cilvēkiem mainīt uzvedību un atturēt viņus no sava viedokļa paušanas. Tādējādi tiek pārkāpta viņu vārda brīvība. Turklāt, ja cilvēki, zinot, ka viņi tiks novēroti, nevēlas apmeklēt demonstrācijas, tas nopietni ietekmē arī pulcēšanās

290 ES Pamattiesību aģentūra, ECT, EP, EDAU (2018), Rokasgrāmata.

291 EDPS (2018), Opinion 3/2018.

292 Andrews, E. L. (11 June, 2020). Governments Aren't Yet Serious About AI's Risk to Human Rights. *Stanford University Human-Centered Artificial Intelligence.* https://hai.stanford.edu/news/governments-arent-yet-serious-about-ais-risk-human-rights

293 Kelly, E. (21 January, 2020). EU makes move to ban use of facial recognition systems. *Science / Business.* https://sciencebusiness.net/news/eu-makes-move-ban-use-facial-recognition-systems; Ulmer, A., Siddiqui, Z. (17 February, 2020). India's use of facial recognition tech during protests causes stir. *Reuters.* https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ

brīvību. Sejas atpazīšanas tehnoloģiju ieviešana var atturēt cilvēkus no pulcēšanās un biedrošanās, baidoties no iespējamām negatīvajām sekām. Tādējādi tiešā veidā tiek ietekmēta arī līdzdalības demokrātijas efektīva darbība.[294]

3.6. Sabiedrības kopējā vērtība

Privātumu bieži saprot kā tiesības, kas aizsargā "privāto", nevis "publisko" sfēru. Tehnoloģijas ir radikāli mainījušas to, kas mūsu ikdienas dzīvē ir privāts un kas publisks. Tiesību zinātnieku vidū šobrīd arvien populārāks kļūst uzskats, ka privātums ir kolektīvs sociāls labums, kā, piemēram, tīrs gaiss un ūdens.[295]

Vēsturiski cilvēku saskarsme bijusi lokāla un īslaicīga. Tikai tuvumā esošie varēja to redzēt, un reiz izteiktie vārdi laika gaitā pazuda. Šobrīd līdz ar interneta un tehnoloģiju attīstību cilvēku mijiedarbība un citu iespējas to novērot var izplatīties telpā un pastāvēt ilgstoši laikā. Mūsu personiskā, profesionālā un finansiālā mijiedarbība aizvien biežāk notiek tiešsaistē, kur gandrīz viss tiek arhivēts un tādējādi potenciāli pastāvīgi meklējams un publicējams.[296] Atteikšanās no sociālo mediju izmantošanas var šķist aizdomīga, jo pastāv uzskats, ka visi cilvēki vēlas savstarpēji mijiedarboties, izmantojot dažādas lietotnes un platformas.

Informācijas un komunikācijas tehnoloģijas ir mainījušas privātuma jēdzienu. Arvien grūtāk ir atšķirt privāto un publisko. Šķiet pilnīgi acīmredzami, ka pāreja uz mazāku privātumu ir neizbēgama un neapturama. Privātuma vērtība saskaras ar jauniem apdraudējumiem līdz ar interneta pieaugumu, vieglumu, ar kādu tas ļauj iegūt, apstrādāt, koplietot un publicēt privāto informāciju, kā arī ar ātro jauno tehnoloģiju attīstību, kas ļauj veikt uzmācīgas novērošanas darbības.

"Publiskās" un "privātās" sfēras nošķiršana liek skatīt privātumu kā individuālas tiesības, kas pastāv līdzās plašākai sabiedrībai. Šis tradicionālais liberālais uzskats, kas balstās uz personības, individualitātes un autonomijas aizsardzību, neskata privātumu kā "sociālu labumu". Netiek ņemta vērā privātuma plašāka sociālā nozīme.[297] Tomēr, lai gan privātums ietver šos principus, tas ir plašāks.

Privātums kalpo nevis tikai indivīda interesēm, bet arī vispārējiem, sabiedrības un kolektīviem mērķiem.[298] Priscila Rīgena (*Priscilla Regan*) skaidro, ka, ska-

294 Sk. FRA (2019), Facial recognition technology.

295 Edwards (2019), *Law, Policy, and the Internet*, p. 53; sk. arī Tzanou (2019), *The Fundamental Right to Data Protection*, pp. 9–10.

296 Donath (2020), Privacy and Public Space.

297 Sk. Moreham, N. A. (2006). Privacy in Public Places. *Cambridge Law Journal*, 65(3), p. 606. https://doi.org/10.1017/S0008197306007240

298 Regan, P. M. (2009). *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill, NC: The University of North Carolina Press, p. 213, 321.

tot privātumu kā individuālas tiesības, politikas veidotājiem ir jāpanāk līdzsvars starp konkurējošām interesēm vai tiesībām, piemēram, tādām sabiedrības interesēm kā drošības aizsardzība. Tomēr sabiedrībai nav jāizvēlas starp dažādām vērtībām un pamattiesībām, tai ir tiesības uz visu pamattiesību nodrošināšanu. Cilvēkiem nav jāizvēlas starp privātuma un datu aizsardzību, no vienas puses, un nacionālo un sabiedrisko drošību, no otras puses. Tāpat kā sabiedrībai nav jāizvēlas starp veselības aizsardzību un privātumu vai demokrātiju. Valstij, ieviešot atbilstošus valsts vai sabiedrības drošības aizsardzības pasākumus, ir jāaizsargā visas cilvēktiesības.

Privātums ir sabiedriska vērtība, tāpēc ka tā aizsargā indivīdu "sabiedrības labā".[299] Privātums nav tikai individuālas tiesības, tās ir grupas tiesības. Tās vairāk pieder grupai kopumā, nevis katram atsevišķam indivīdam.[300] Visai sabiedrībai, ne tikai indivīdam ir labāk, ja pastāv privātums. Lai gan mēs visi esam ieinteresēti privātuma saglabāšanā, tomēr to var apdraudēt liels daudzums individuālu izvēļu, un to apliecina sociālo mediju platformu un dažāda veida lietotņu arvien plašāka izmantošana.[301]

Viens no biežāk dzirdētajiem satraukuma iemesliem ir, ka jaunās tehnoloģijas piespiedīs mūs atteikties no privātuma. ASV tehnoloģiju giganti kļūst daudz varenāki nekā valstis. Mēs ļaujam tiem piekļūt mūsu personiskajai informācijai, ko nekad nedotu nevienai valsts iestādei, – mēs neļautu valdībai ievietot kameras un mikrofonus savās mājās vai izsekot mūsu atrašanās vietu ierīcēs. Šie tehnoloģiju uzņēmumi iegūst informāciju par lietotājiem, lai prognozētu un ietekmētu mūsu uzvedību. Mēs arvien vairāk un vairāk paļaujamies uz mākslīgā intelekta rezultātiem, kas tiek atlasīti pēc konkrētiem algoritmiem, ņemot vērā mūsu pašu sniegto informāciju par mūsu vēlmēm, interesēm u. tml. Tomēr šī piedāvātā un atlasītā informācija var neparādīt mums vairāk atbilstošu un svarīgāku informāciju. Vēl jo vairāk, mākslīgā intelekta algoritmi var ļaut analizēt, saprast un ietekmēt arī mūsu domas un jūtas. Lielajiem tehnoloģiju uzņēmumiem, piemēram, "Facebook", kas veic profilēšanu reklāmas nolūkos, nav nekādas intereses par katru konkrēto lietotāju, un to darbības ne tik daudz uzreiz tieši aizskar katru no mums personiski, kā tiek mēģināts arvien vairāk atņemt visu lietotāju kā grupas tiesības. Privātums paredz aizsardzību pret šādu manipulāciju, turklāt nevis

299 Solove (2009), *Understanding Privacy*, pp. 92–93. Sk. arī Tzanou (2019), *The Fundamental Right to Data Protection*, p. 10.

300 Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy and Technology*, 27, pp. 1–3. https://doi.org/10.1007/s13347-014-0157-8. Vairāk par grupu privātumu sk. Taylor, L., Floridi, L., van der Sloot, B. (eds.). (2017). *Group Privacy: New Challenges of Data Technologies*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8.

301 Edwards (2019), *Law, Policy, and the Internet*, p. 53.

katram no mums atsevišķi, bet kā visu lietotāju grupai. Lai varētu aizsargāt katru no mums atsevišķi, ir jāaizsargā visas sabiedrības kopējās intereses.

Tiesību zinātnieki Lineta Teilore (*Linnet Taylor*), Lučāno Florīdi (*Luciano Floridi*) un Bārts van der Slots (*Bart van der Sloot*) norāda, ka jaunās datu tehnoloģijas, kas ļauj masveidā pārtvert un analizēt datus, kategorizēt cilvēkus bez viņu ziņas un neredzami novērot personu grupu kustību un darbību, rada jautājumus, kuri pārsniedz individuālā privātuma kaitējuma līmeni un rodas grupai gan apzinoties, gan nezinot. Grupas privātumu var uzskatīt par svarīgu individuālā privātuma papildinājumu, un, lai grupas privātums kļūtu par jēdzienu, kam var būt nozīme privātuma un datu aizsardzības tiesībās, mums, iespējams, būtu jāsāk no īpašu problēmu risināšanas. Viena no tām ir masveida novērošana.[302]

Lai demokrātija būtu spēcīga, iedzīvotājiem ir jābūt kontrolei pār saviem personas datiem. Filozofe Karisa Velisa (*Carissa Véliz*) grāmatā "Privātums ir vara" (*Privacy is Power* – angļu val.) uzsver, ka vara, ko privātums mums piešķir kā pilsoņiem, ir nepieciešama demokrātijai – lai mēs varētu balsot atbilstoši savai pārliecībai un bez ietekmēšanas, lai mēs varētu anonīmi protestēt, nebaidoties no sekām, lai mums būtu brīvība apvienoties un paust savas domas. Ja vēlamies dzīvot demokrātijā, varai ir jāpieder cilvēkiem. Un, kam ir dati, tam ir vara. Ja lielākā daļa varas pieder uzņēmumiem, mēs dzīvosim sabiedrībā, kuru pārvalda turīgie. Ja lielākā daļa varas pieder valstij, mums būs sava veida autoritārisms. Lai pārvaldes vara būtu likumīga, tai ir jābalstās uz cilvēku piekrišanu, nevis uz viņu datiem. Liberālā demokrātija nav pašsaprotama, tā ir kaut kas tāds, ar ko mums katru dienu jācīnās. Privātums ir svarīgs, jo tas cilvēkiem dod varu. Privātums ir sabiedrisks labums, un to aizsargāt ir mūsu pilsoniskais pienākums.[303] Tomēr vispirms katram cilvēkam ir jāapzinās, ka viņam šī vara pieder.

3.7. Privātuma nozīmes apzināšanās

Tehnoloģiju uzņēmumi, kas izmanto milzīgus datu apjomus un kļūst arvien spēcīgāki, ir mēģinājuši no jauna definēt privātumu un pārliecināt cilvēkus par privātuma vērtības samazināšanos. Tam pamatā ir peļņa, ko tie gūst, patvaļīgi un neatļauti izmantojot personu datus.

1999. gadā "Sun Microsystems" izpilddirektors Skots Maknīlijs (*Scott McNealy*) atzina: "[Jums] jebkurā gadījumā ir nulle privātuma." Pēc desmit gadiem,

302 Sk. Taylor, L., van der Sloot, B., Floridi, L. (2017). Conclusion: What Do We Know About Group Privacy? In: Linnet, T., Floridi, L., van der Sloot, B. (eds.). *Group Privacy*, pp. 233, 236. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8_12

303 Véliz (2021), *Privacy Is Power*, p. 82.

2010. gadā, šo viedokli dedzīgi atbalstīja divi tehnoloģiju giganti. "Facebook" izpilddirektors Marks Zakerbergs (*Mark Zuckerberg*) skaidroja: "Cilvēki patiešām ir akceptējuši ne tikai dalīšanos ar vairāk un dažāda veida informāciju, bet arī atklātāk un ar vairākiem cilvēkiem. Šī sociālā norma attīstījusies laika gaitā."[304] Tajā pašā gadā "Google" izpilddirektors Ēriks Emersons Šmits (*Eric Emerson Schmidt*) paziņoja: "Ja ir kaut kas tāds, ko nevēlaties, lai kāds zinātu, varbūt jums to nemaz nevajadzētu darīt."[305]

Šo uzņēmumu publiskais vēstījums tagad ir kļuvis gluži pretējs. 2020. gada Pasaules Ekonomikas forumā Davosā Šveicē "Google" izpilddirektors Sundars Pičai (*Sundar Pichai*) apgalvo, ka privātums "nevar būt luksusa prece" un ka atbalsta valdību privātuma regulējumu.[306] Rodas jautājums, kādi notikumi ir noveduši pie šīs attieksmes maiņas.

Galvenais iemesls, kas var ietekmēt privātuma virzienu, ir izpratnes veicināšana par privātumu un personas datu izmantošanu. Atbalsts privātumam vienmēr palielinās, vairāk apzinoties ar privātumu un datu aizsardzības neatļautu izmantošanu un pārkāpumiem saistītos jautājumus. Mēs varam īpaši pateikties tiem cilvēkiem, kuri ir kļuvuši slaveni ar to, ka "izgaismojuši", kā gan valsts institūcijas, gan privātie uzņēmumi, īpaši ASV tehnoloģiju giganti, ļaunprātīgi izmanto personas datus.

Viens no šādiem cilvēkiem, kas būtiski ietekmējis privātuma virzienu, ir Edvards Snoudens, kurš 2013. gada jūlijā atklāja ASV masveida novērošanas programmas neiedomājamos apmēros. Šīs atklāsmes izraisīja globālu sašutumu, kā arī ietekmi uz ES datu aizsardzības sistēmu, paātrinot tās reformu.[307]

Būtiska nozīme stingru datu aizsardzības prasību izstrādē ir EST, kas ir pieņēmusi svarīgus spriedumus lietās, kas ir ietekmējušas datu aizsardzības tiesību attīstību ES. Divas no šādām lietām, kas satricināja visu ES datu nodošanas sistēmu, EST nonāca, pateicoties Maksimiliāna Šrema (*Maximilian Schrems*) iesniegtajām sūdzībām. 2013. gadā viņš iesniedza sūdzību Īrijas datu aizsardzības iestādē

304 The Facebook CEO Chellenges the social norm of Privacy. (12 January, 2010). *Reuters.* https://www.reuters.com/article/urnidgns852573c400693880002576a80069db04/facebook-ceo-challenges-the-social-norm-of-privacy-idUS174222527820100112

305 Jennings, R. (11 December, 2009). Google CEO: if you want privacy, do you have something to hide? *Computerworld*. https://www.computerworld.com/article/2468308/google-ceo--if-you-want-privacy--do-you-have-something-to-hide-.html

306 Google CEO backs GDPR, says privacy should not be a luxury. (22 January, 2020). *The Institute of Engineering & Technology.* https://eandt.theiet.org/content/articles/2020/01/google-ceo-backs-gdpr-says-privacy-should-not-be-a-luxury/

307 Pēc 2013. gada atklājumiem vairāk nekā 1000 akadēmiskās sabiedrības pārstāvju parakstīja dokumentu, lai iebilstu pret masveida novērošanu: Sterling, B. (17 January, 2014). Academics Against Mass Surveillance. *WIRED*. https://www.wired.com/2014/01/academics-mass-surveillance/

par "Facebook" veikto datu nodošanu uz ASV, uzskatot, ka ASV nacionālās drošības regulējums nenodrošina pietiekamu ES pilsoņu personas datu aizsardzību. EST "Schrems I" lietā 2015. gadā atzina par neatbilstošu un spēkā neesošu datu nodošanas mehānismu starp ES un ASV, respektīvi, Eiropas Komisijas lēmumu par aizsardzības līmeņa pietiekamību datu nodošanai uz ASV kā trešo valsti jeb tā saukto drošās zonas lēmumu, ņemot vērā, ka ASV prakse attiecībā uz datu iegūšanu no privātiem uzņēmumiem nacionālās drošības nolūkos nav atbilstoša Hartai. 2020. gada 16. jūlija spriedumā "Schrems II" lietā EST izvērtēja Eiropas Komisijas 2016. gadā pieņemto jauno atbilstības lēmumu 2016/1250 jeb tā saukto ASV un ES privātuma vairogu (*EU-U.S. Privacy Shield* – angļu val.) un atkārtoti atzina lēmumu par spēkā neesošu, ņemot vērā ASV novērošanas regulējumu. Minētās lietas detalizētāk aplūkotas grāmatas piektajā nodaļā.

Iespējams, vēl vairāk privātuma apzināšanos, kā arī nepieciešamību pēc jauna tiesiskā regulējuma veicināja "Facebook" un "Cambridge Analytica" skandāls. Ja Snoudena atklājumi parādīja, kādā veidā valsts iestādes var prettiesiski izmantot personu datus, tad "Cambridge Analytica" skandāls atklāja, cik negatīvas sekas var radīt lielo tehnoloģiju uzņēmumu un sociālo mediju veiktā personas datu apstrāde, ja tā netiek regulēta un uzraudzīta. Apvienotajā Karalistē reģistrēts datu profilēšanas uzņēmums "Cambridge Analytica" 2018. gada sākumā bez piekrišanas izmantoja miljoniem "Facebook" lietotāju datus, lai ar konkrētai auditorijai mērķētām politiskām reklāmām ietekmētu vēlētāju izvēli, to skaitā 2016. gada *Brexit* referenduma kampaņas un ASV prezidenta Donalda Trampa (*Donald John Trump*) priekšvēlēšanu kampaņas laikā. Šie notikumi skaidri parādīja, cik būtisku kaitējumu demokrātijai un sabiedrībai var nodarīt dezinformācija sociālajos medijos, izplatot nepatiesu, neprecīzu un maldinošu informāciju, lai ietekmētu iedzīvotāju politiskos, kā arī cita veida uzskatus un izvēles.[308]

Pēc šī skandāla sabiedrība arvien uzstājīgāk sāka pieprasīt sociālo mediju gigantu atbildību, datu aizsardzības prasību ievērošanu, pārredzamu un viegli saprotamu lietotāju informēšanu par datu apstrādi utt. Eiropas Komisija izveidoja speciālo komisiju, lai izskatītu "Cambridge Analytica" lietu un vairākkārt nopratināja Marku Zakerbergu. "Facebook" apliecināja, ka aptuveni 2,7 miljonu Eiropas iedzīvotāju dati ir izmantoti saistībā ar šo skandālu. Apvienotās Karalistes datu aizsardzības uzraudzības iestāde ICO piemēroja 500 000 eiro naudas sodu, ko

308 Marsden, C., Meyer, T. European Parliament. Panel for the Future of Science and Technology. European Science Media-Hub. (2019). Regulating Disinformation with Artificial Intelligence: Effects of Disinformation Initiatives on Freedom of Expression and Media Pluralism. European Union. https://data.europa.eu/doi/10.2861/003689

"Facebook" piekrita samaksāt.[309] Itālijas uzraudzības iestāde savukārt piemēroja sociālo mediju milzim sodu viena miljona eiro apmērā.[310] Aktīvi tiek meklēti risinājumi un izvērtēti jauna tiesiskā regulējuma priekšlikumi, lai sociālajos medijos cīnītos pret dezinformāciju un nepieļautu turpmāku manipulāciju ar vēlēšanām.

Līdzās arvien pieaugošajai milzīgo tehnoloģiju uzņēmumu varai būtiskākais privātumu apdraudošais aspekts ir jaunās uz datu analīzi balstītās tehnoloģijas, īpaši novērošanas tehnoloģijas. Bieži vien var dzirdēt satraukumu, ka jaunās tehnoloģijas, kā mākslīgais intelekts un lietu internets, piespiedīs mūs atteikties no privātuma. Visplašākās diskusijas ir radījušas jau iepriekš aplūkotās sejas atpazīšanas tehnoloģijas.

Ja līdz šim privātuma un datu aizsardzības prasības bieži vien tika uztvertas negatīvi, norādot, ka tās kavē un traucē tehnoloģiju attīstību, līdz ar sabiedrības arvien plašāku uzmanību un interesi arī uzņēmumu attieksme pret regulējumu ir mainījusies. Tehnoloģiju uzņēmumu darbības pamatā ir patērētāju uzticība. Ja pakalpojumiem un precēm nebūs uzticības, lietotāji tos neiegādāsies un neizmantos. Daudzi lielie tehnoloģiju uzņēmumi ir ne tikai sākuši paust atbalstu privātumam, bet arī paši prasīt valdībām pieņemt regulējumu.[311] Šādas attieksmes maiņas iemesli var būt vēlēšanās stiprināt savu dominanci un varu.[312] Tomēr nav noliedzams – ja vēlas, lai cilvēki izmanto tehnoloģijas, ir jāpanāk, ka viņi tām uzticas. Regulējums ir viena no iespējām, kā šo uzticību iespējams panākt.

3.8. Krīze kā satricinājums privātumam

Nekādi citi notikumi nevar vairāk veicināt jaunu pamattiesības ierobežojošu pasākumu ieviešanu kā krīzes situācijas. Krīzes laikā, kad tiek apdraudētas tādas vērtības kā drošība un veselība, iedzīvotājus ir visvieglāk pārliecināt, ka ir nepieciešams piemērot pasākumus, kas var būtiski ierobežot viņu pamattiesības, tai

309 Statement on an agreement reached between Facebook and the ICO. (30 October, 2019). *WIRED.* https://www.wired-gov.net/wg/news.nsf/articles/Statement+on+an+agreement+reached+between+Facebook+and+the+ICO+30102019151000?open

310 Dobber, T., Fathaigh, R. Ó., Zuiderveen Borgesius, F. J. (2019). The regulation of online political micro-targeting in Europe. *Internet Policy Review*, 8(4). https://doi.org/10.14763/2019.4.1440

311 Nickelsburg, M. (21 January, 2020). Microsoft President Brad Smith calls for AI regulation at Davos. *GeekWire.* https://www.geekwire.com/2020/microsoft-president-brad-smith-calls-ai-regulation-davos/; Sherman, J. (28 Januar, 2020). Oh Sure, Big Tech Wants Regulation—on Its Own Terms. *WIRED.* https://www.wired.com/story/opinion-oh-sure-big-tech-wants-regulationon-its-own-terms/

312 Kharpal, A. (28 January, 2020). Big Tech's calls for more regulation offers a chance for them to increase their power. *CNBC.* https://www.cnbc.com/2020/01/28/big-techs-calls-for-ai-regulation-could-lead-to-more-power.html

skaitā tiesības uz privātumu un datu aizsardzību. Ja vienos svaru kausos tiek likts privātums, bet otros – sabiedrības drošība vai veselība, tie vienmēr nosvērsies par labu otrajiem. Sabiedrība vienmēr būs gatava atteikties no privātuma, lai aizsargātu tādas pamatvajadzības kā drošība un veselība.

Kā norāda Liliana Edvardsa, iespējams, viens no lielākajiem globālajiem izaicinājumiem datu aizsardzībai un privātumam ir baiļu, novērošanas un drošības kultūras veidošanās, ko izraisīja ASV šausminošie 11. septembra terorakti, pēc kuriem NSA ieviesa elektronisko sakaru uzraudzības programmu. Arī Eiropas Savienībā nepieciešamība apkarot terorismu iepriekš bija pamatā datu saglabāšanas režīma ieviešanai, kas ļāva valstīm uzraudzīt sakarus drošības nolūkos. Reaģējot uz teroristu uzbrukumiem vairākās valstīts, ES pieņēma Datu saglabāšanas direktīvu par spīti kritikai, ka tā neatbilst cilvēktiesībām. Direktīva ļāva valstīm uzraudzīt sakarus drošības nolūkā. Pagāja astoņi gadi, līdz šo direktīvu atcēla EST. Vēsturiskā pieredze liecina, ka krīzes un satricinājumu laikā pieņemtus pamattiesības ierobežojošus pasākumus vēlāk ir ļoti grūti atcelt un tas var prasīt ilgu laiku. Lai veicinātu novērošanas kultūras attīstību, tiek izmantoti ne tikai terorakti un drošības draudi.

Lielu pārbaudījumu un satricinājumu visās jomās, to skaitā cilvēktiesībām un privātumam, neapšaubāmi radīja arī Covid-19 pandēmijas izraisītā globālā krīze. Kā atklāja grāmatas pirmajā nodaļā aprakstītie piemēri, sabiedrības bailes par personisko drošību un veselību, kā arī vispārējo haosu, neaizsargātību un nedrošību gan valsts iestādes, gan privātie uzņēmumi izmantoja, lai lielā ātrumā izstrādātu un ieviestu daudzas jaunas digitālās novērošanas tehnoloģijas. Turklāt daudzos gadījumos šīs tehnoloģijas tika ieviestas, neizvērtējot to efektivitāti, nepieciešamību un samērīgumu.

Jautājumus par Covid-19 krīzes laikā piemēroto ierobežojošo pasākumu, tostarp jauno novērošanas tehnoloģiju, risinājumiem, to likumību un atbilstību cilvēktiesībām tiesas izvērtēs vēl ilgi pēc pandēmijas beigām. Lai gan krīzes situācijā ir pieļaujams vairāk ierobežot personu pamattiesības, šādiem ierobežojumiem ir jābūt samērīgiem un pamatotiem, un tie ir jāpārtrauc, tiklīdz situācija uzlabojas. Tajā pašā laikā sagaidāms, ka valsts iestādes un privātais sektors turpinās attīstīt un nevēlēsies atteikties no jau ieviestajām novērošanas tehnoloģijām.

Jebkura krīze nozīmē pārmaiņas. Arī pēc Covid-19 pandēmijas pasaule būs pavisam citāda nekā tā, kurā mēs dzīvojām iepriekš. Nav paredzams, cik daudz Covid-19 krīze izmainīs sabiedrību, kā arī tās ietekmi uz cilvēktiesībām un to ierobežošanu. Tomēr būtu naivi domāt, ka ieviestie cilvēktiesības ierobežojošie, tostarp novērošanas, pasākumi pilnīgi pazudīs un valstis atkal atgriezīsies pie iepriekšējās kārtības. Lai veicinātu pasākumu atbilstību un likumību, vispirms ir svarīgi apzināties to ietekmi uz pamattiesībām, kā arī uz visu sabiedrību un demokrātiju, kā arī pēc tam izstrādāt atbilstošu regulējumu, kas novērstu šo apdraudējumu.

Grāmatā iepriekš atklāts, kā mākslīgā intelekta novērošanas tehnoloģijas ietekmē cilvēktiesības, kā arī demokrātiju un sabiedrību kopumu. Šī nodaļa parāda, ka, lai gan viedokļi par to, kāpēc privātums ir jāaizsargā, ir dažādi un laika gaitā mainās un attīstās, tomēr privātumam ir būtiska un patstāvīga nozīme. Tiesības uz privātumu vēsturiski ir attīstījušās kā būtiskas liberālas tiesības, kas nodrošina aizsardzību pret varas ļaunprātīgu izmantošana; tiesības palikt vienam, tiesības kontrolēt informāciju par sevi – tās ir autonomijas un rīcības brīvības garants. Privātums tiek uztverts arī kā visas sabiedrības kopīga vērtība un kā cilvēka cieņas neatņemams elements, kas kā ētikas pamatvērtība jauno tehnoloģiju laikmetā aizsargā pret visaptverošu novērošanu un varas asimetriju. Tādējādi tiesības uz privātumu ir uzskatāmas gan par pamattiesībām, gan ētikas principu un sabiedrisku vērtību. Tās ir arī būtisks tiesiskuma un demokrātijas elements.

Vēl vienas pamattiesības, ko būtiski ietekmē mākslīgā intelekta novērošanas tehnoloģijas un kas ir cieši saistītas ar tiesībām uz privātumu, ir tiesības uz datu aizsardzību. Šīs abas pamattiesības izvirza konkrētas prasības un aizsardzības garantijas, kas piemērojamas arī mākslīgā intelekta novērošanas sistēmām. Turklāt datu aizsardzības tiesības ir galvenais regulējums, kas jau šobrīd piemērojams attiecībā uz mākslīgā intelekta sistēmām un kas būtiski ietekmē arī topošo mākslīgā intelekta tiesisko regulējumu, kuru šobrīd aktīvi izstrādā gan ES, gan citas starptautiskās organizācijas. Nākamajā nodaļā apskatīta tiesību uz datu aizsardzību tiesiskā regulējuma attīstība, kā arī mākslīgā intelekta regulējuma aizsākumi gan starptautiskā, gan ES līmenī.

4. DAĻA

Datu aizsardzības tiesības un mākslīgā intelekta regulējuma attīstība

Datu aizsardzības aizsākumu pamatā ir tehnoloģiju progress. Līdz ar informācijas sabiedrības un tehnoloģiju attīstību datu aizsardzības tiesības kā patstāvīgas cilvēktiesības pakāpeniski izveidojās no tiesībām uz privāto dzīvi.

Eiropā tās sāka attīstīties 20. gadsimta 70. gadu sākumā, kad līdz ar tehnoloģiju straujo progresu arvien plašāk sāka izmantot datorus un bija nepieciešams izstrādāt noteikumus, kas regulētu personīgās informācijas vākšanu un apstrādi.[313] Mūsdienās datu aizsardzības tiesiskais regulējums ir pieņemts lielākajā daļā pasaules valstu, kā arī daudzās valstīs privātums un datu aizsardzība ir konstitucionāli garantētas tiesības. Kā liecina ANO sniegtā informācija, 132 no 194 valstīm ir pieņēmušas tiesību aktus par datu aizsardzību un privātumu.[314]

Līdzās valstu tiesiskajam regulējumam arī ES un starptautiskā līmenī ir pieņemti daudzi datu aizsardzības tiesiskie instrumenti. Atšķirīgais valstu regulējums un dažādie standarti attiecībā uz datu iegūšanu, izmantošanu un nodošanu radīja būtiskus šķēršļus starptautiskiem uzņēmumiem, tāpēc bija nepieciešams vienoties par starptautiski vienotu risinājumu, kurā tiktu samērotas, no vienas puses, personas tiesības uz datu aizsardzību un, no otras puses, uzņēmumu komerciālās intereses. Izveidojās divas galvenās pieejas, kādā tiek skatītas datu aizsardzības tiesības: 1) ekonomiskā pieeja un 2) cilvēktiesību aizsardzības pieeja.[315] Tās abas apskatītas nodaļas turpinājumā.

Datu aizsardzības regulējums ir attīstījies, mēģinot atrast veidu, kā samērot dažāda veida intereses: uzņēmumu biznesa intereses, īpaši tehnoloģiju nozarē; valsts iestāžu intereses aizsargāt valsts un sabiedrības drošību, kā arī citas sabiedrības intereses; preses un izteiksmes brīvība; publisko iestāžu intereses dalīties ar datiem, lai digitalizētu dažāda veida publiskos pakalpojumus, piemēram, transporta, veselības, nodokļu jomā, utt.[316] Lai gan šajā pētījumā pamatā ir analizēts, kā privātums un datu aizsardzība saduras un ir samērojamas ar valsts un sabiedrības drošības interesēm, piemērojot dažāda veida novērošanas pasākumus, kā šī

313 Rudgard, S. (2018). Origins and Historical Context of Data Protection Law. In: Ustaran, E., Lovells, H. (eds.), *European Data Protection. Law and Practice.* International Association of Privacy Professionals (IAPP), pp. 20, 26.

314 Sk. UNCTAD. Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

315 Tzanou (2019), *The Fundamental Right to Data Protection*, p. 14.

316 Edwards (2019), *Law, Policy, and the Internet*, p. 66.

interešu sadursme attīstās un ir regulējama mākslīgā intelekta laikmetā, tomēr piemērojamais regulējums, kā arī prakse daudzos gadījumos var būt līdzīgā veidā attiecināma, izvērtējot arī citus interešu konfliktus.

Datu aizsardzības tiesības iezīmē sākumu informācijas un komunikāciju tehnoloģiju regulējumam no likumdevēja puses. Tiesiskie instrumenti, kas tika izveidoti, balstoties uz 20. gadsimta 70. un 80. gados definētajiem principiem, vairs nespēja reaģēt uz sociāli tehniskajām izmaiņām. Arvien plašākas datu pārsūtīšanas iespējas, jaunie datu glabāšanas un skaitļošanas resursi, īpaši mākoņdatošana, lielākās daļas mūsu dzīves un vides pakāpeniska datu apstrāde, sevišķi līdz ar lietu interneta pieaugumu, kā arī liela mēroga un prognozējoša datu analīze, pamatojoties uz lielajiem datiem un mašīnmācīšanos, radīja nepieciešamību pēc jauna regulējuma.[317] Lai reaģētu uz šīm pārmaiņām, Eiropā tika veikta datu aizsardzības reforma, kuras rezultātā ES pieņēma VDAR un citus tiesību aktus, kā arī Eiropas Padome modernizēja Konvenciju 108.[318]

Tajā pašā laikā regulējuma izstrādes un pieņemšanas process vienmēr aizņem ilgu laiku, līdz ar to neizbēgami tas nespēj tikt līdzi straujajai tehnoloģiju attīstībai. Kā atklāts grāmatas sestajā nodaļā, jaunais datu aizsardzības regulējums nespēj risināt daudzus izaicinājumus, ko rada mākslīgā intelekta sistēmas un citas jaunās tehnoloģijas un tiešsaistes platformas.

Pēdējo gadu laikā gan starptautiskā un ES, gan nacionālā līmenī ir pieņemti daudzi nesaistoši dokumenti, kas cenšas šo "plaisu" starp regulējumu un tehnoloģiju attīstību novērst, kā arī tiek izstrādāti daudzi priekšlikumi, kā uzlabot esošo regulējumu. Arī privātie uzņēmumi, tehnoloģiju organizācijas un nevalstiskās organizācijas aktīvi iesaistās diskusijās par mākslīgā intelekta sistēmu regulēšanu un ir pieņemtas dažāda veida deklarācijas un vadlīnijas, kas nosaka mākslīgā intelekta principus. Pašregulācija nav pietiekama, lai nodrošinātu, ka privātās organizācijas izstrādā un izmanto mākslīgā intelekta sistēmas ētiski un atbilstoši sabiedrības interesēm, un noteiktu to atbildību. Skaidrs regulējums ir jāpieņem arī attiecībā uz publisko sektoru un privātā un publiskā sektora partnerību. Eiropas un starptautiskās organizācijas šobrīd aktīvi izstrādā jaunu regulējumu, kas paredzētu juridiski saistošas prasības mākslīgā intelekta sistēmām un citām jaunajām tehnoloģijām un platformām.

Nodaļas turpinājumā aplūkots, kā starptautiskās organizācijas – Eiropas Padome, OECD, ANO, UNESCO – ir attīstījušas datu aizsardzības tiesības. Pēc tam aplūkota ES datu aizsardzības regulējuma attīstība, kur tiesības uz datu aizsardzību atšķirībā no citu starptautisko organizāciju pieņemtajiem cilvēktiesību dokumentiem

317 Mantelero (2020), Regulating AI within the Human Rights Framework, p. 484.

318 Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi. Pieņemta 28.01.1981. (EP, Latvijā spēkā no 01.09.2001.). *Latvijas Vēstnesis*, 12.04.2001., Nr. 59.

ir noteiktas kā atsevišķas pamattiesības. Vienlaikus nodaļā sniegts vispārīgs pārskats, kā dažādas organizācijas ir iesaistījušās diskusijā par masveida novērošanas pasākumu apdraudējumu cilvēktiesībām un kā pakāpeniski tiek izveidots mākslīgā intelekta regulējums, apskatot būtiskākās iniciatīvas starptautiskā un ES līmenī.

4.1. Starptautiskās iniciatīvas

4.1.1. Eiropas Padome

Eiropas Padome ir izstrādājusi vienotus Eiropas cilvēktiesību aizsardzības standartus, kā arī radījusi efektīvu to aizsardzības mehānismu.[319] Viens no būtiskākajiem starptautiskajiem cilvēktiesību dokumentiem ir ECTK, kuras ievērošanu uzrauga ECT. 1968. gadā Eiropas Padomes Parlamentārā asambleja uzdeva Ministru komitejai izvērtēt, vai valstu regulējums pietiekami aizsargā tiesības uz privātumu pret pārkāpumiem, ko var radīt moderno zinātņu un tehnoloģiju attīstība, un, ja atbilde ir negatīva, izstrādāt rekomendācijas, lai labāk aizsargātu tiesības uz privātumu.[320] Eiropas Padomes Ministru komiteja pieņēma divas rezolūcijas par datu aizsardzību: 1973. gadā rezolūcija noteica datu aizsardzības principus privātajā sektorā, bet 1974. gada rezolūcija – publiskajā sektorā.[321] Rezolūcijas ieteica nacionālajā likumdošanā ietvert prasības, kas arī tagad lielākoties ir pamatā datu aizsardzības principiem, piemēram, lai dati tiktu iegūti godīgi, lai tiktu nodrošināta to precizitāte un aktualitāte, lai tiktu ievērots datu minimizēšanas princips, kas aizliedz vākt vairāk datus un glabāt tos ilgāk, nekā tas ir nepieciešams, pienākums uzraudzīt to izpaušanu, datu subjektu tiesības utt. Tajā pašā laikā rezolūcijas nenoteica pasākumus, kas valstīm būtu jāveic, lai ieviestu principus nacionālajā likumdošanā. Lai saskaņotu valstu tiesību aktus, kas tika strauji pieņemti,

319 Sk. Pati, R. (2009). Due Process and International Terrorism. Leiden, Boston: Nijhoff, pp. 72, 73; Christoffersen, J. and Madsen, M. R. (2011). Introduction: The European Court of Human Rights between Law and Politics. In: Christoffersen, J. and Madsen, M. R. (eds.), *The European Court of Human Rights between Law and Politics*. Oxford: Oxford University Press, p. 2.

320 Parliamentary Assembly of the Council of Europe. (1968). Recommendation 509. Human rights and modern scientific and technological developments. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en

321 Council of Europe. Committee of Ministers. (1974). Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51; Council of Europe. Committee of Ministers. (1973). Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830

Eiropas Padome uzsāka darbu pie viena no nozīmīgākajiem starptautiskajiem tiesiskajiem instrumentiem.

1981. gadā Eiropas Padome pieņēma Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (Konvencija 108).[322] Šī konvencija ir pirmais un līdz šim brīdim vienīgais juridiski saistošais starptautiskais dokuments datu aizsardzības jomā, kuram var pievienoties ikviena pasaules valsts, arī valstis ārpus Eiropas Padomes. Konvencijai ir pievienojušās 55 valstis – visas Eiropas Padomes dalībvalstis (46 valstis), kā arī to ir ratificējušas vairākas valstis ārpus Eiropas.[323]

Konvencija 108 tika pieņemta, lai nodrošinātu pamattiesību un pamatbrīvību, it īpaši privātās dzīves neaizskaramības, ievērošanu, kā arī regulētu automātiski apstrādāto personas datu plūsmu pāri robežām. Tā attiecas uz datu apstrādi gan valsts, gan privātajā sektorā. Konvencijā ir noteikti datu aizsardzības principi. Tā uzliek pienākumu dalībvalstīm pieņemt atbilstošus datu aizsardzības noteikumus, kā arī nosaka datu aizsardzības likumības un datu kvalitātes principu, pienākumu nodrošināt īpašu kategoriju datu aizsardzību, datu drošības principu un apstrādes pārredzamības principu. Konvencijā 108 ir noteiktas datu subjekta tiesības, tostarp tiesības, lai tiktu ņemts vērā personas viedoklis par automatizētu datu apstrādi, tiesības uz informāciju, tiesības iebilst pret datu apstrādi, tiesības piekļūt, labot un dzēst datus, kā arī izmantot tiesiskās aizsardzības līdzekļus datu aizsardzības pārkāpuma gadījumā. Konvencija uzliek datu pārzinim un apstrādātājam pienākumu veikt atbilstošus pasākumus, lai varētu pierādīt datu apstrādes atbilstību Konvencijai. Tā paredz iespēju atkāpties no noteiktām datu aizsardzības prasībām, ja tas ir paredzēts normatīvajos aktos, tiek ievērota pamattiesību un pamatbrīvību būtība un šāda atkāpšanās ir samērīga un nepieciešama demokrātiskā sabiedrībā, lai aizsargātu tādas sabiedrības intereses kā valsts un sabiedriskā drošība, kā arī datu subjektu vai citu personu tiesības un brīvības. Konvencijā ir regulēta arī pārrobežu personas datu nodošana. 2001. gadā tika veikti Konvencijas labojumi, pieņemot papildu protokolu, kas ieviesa noteikumus par pārrobežu datu plūsmu uz trešajām valstīm un noteica obligātu valsts datu aizsardzības uzraudzības iestāžu izveidošanu.

Eiropas Padome 2011. gadā uzsāka darbu pie Konvencijas 108 modernizēšanas, lai nodrošinātu tās efektivitāti, ņemot vērā informācijas un komunikācijas

322 Vairāk par Konvencijas 108 pieņemšanas procesu sk.: Council of Europe. (1981) Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/16800ca434

323 Līdz 2021. gada jūnijam Konvencijai 108 bija pievienojušās šādas valstis, kas nav ES dalībvalstis: Argentīna, Kaboverde, Maurīcija, Meksika, Maroka, Urugvaja, Senegāla un Tunisija. Sk. Council of Europe. Chart of signatures and ratifications of Treaty 108. Status as of 12/06/2021. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures

tehnoloģiju radītos izaicinājumus privātuma aizsardzībai.[324] Konvencijas 108 modernizēšana tika veikta paralēli ES datu aizsardzības reformai, pēc iespējas nodrošinot tiesiskā regulējuma atbilstību.

2018. gada 18. maijā Eiropas Padome pieņēma protokolu[325], ar ko groza Konvenciju 108, un tas tika atvērts parakstīšanai 2018. gada 25. jūnijā (Konvencija 108+). Protokols nostiprina Konvencijā 108 noteiktos datu aizsardzības principus un ietver papildu aizsardzības pasākumus, lai risinātu problēmas, kas saistītas ar personas datu aizsardzību, ko rada jaunās tehnoloģijas. Modernizētā konvencija ievērojami palielina datu aizsardzības līmeni. Tā nosaka stingrākas prasības attiecībā uz proporcionalitātes principu un datu minimizēšanas principu, datu apstrādes likumību un datu apstrādes pārredzamību. Tā paplašina sensitīvo datu veidus, ietverot arī ģenētiskos un biometriskos datus un datus par etnisko izcelsmi. Konvencija 108+ paredz arī jaunus pienākumus, tostarp ziņot par nopietniem datu pārkāpumiem, un nosaka stingrāku datu pārziņa atbildību, kā arī skaidru pārrobežu datu plūsmas režīmu. Turklāt tā piešķir personām jaunas tiesības algoritmisko lēmumu pieņemšanas kontekstā, kas ir īpaši svarīgi saistībā ar mākslīgā intelekta attīstību. Tā arī paplašina Konsultatīvās komitejas kompetenci, kura uzrauga, vai puses efektīvi īsteno atjaunināto līguma noteikumus. Konvencija 108+ nostiprina datu aizsardzības iestāžu pilnvaras un neatkarību, kā arī uzlabo starptautisko sadarbību.

Konvencijā noteiktie principi saskan un pastiprina ES datu aizsardzības tiesisko regulējumu. Pievienošanās Konvencijai 108 tiek ņemta vērā, vērtējot aizsardzības līmeni valstīs ārpus ES, it īpaši starptautisko datu nosūtīšanas gadījumā.[326]

Saistībā ar jautājumu par personas datu apstrādi valsts drošības un aizsardzības nolūkā Konvencijas 108+ 11. pantā ir iekļauta stingra pārbaudes un līdzsvara (*checks and balance* – angļu val.) sistēma. Konvencija 108+ attiecas uz visu personas datu apstrādi publiskajā un privātajā sektorā, ieskaitot drošības un izlūkošanas dienestus (3. pants). Tā paredz piemērot datu aizsardzības principus visām apstrādes darbībām, arī tām, kas veiktas valsts drošības apsvērumu dēļ, ar

324 Vairāk par Konvencijas 108 modernizēšanu sk. Council of Europe. (2018). Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/16808ac91a

325 Protokols, ar ko groza Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu apstrādi: *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Pieņemts 10.10.2018. https://rm.coe.int/16808ac918; Council of Europe. (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data – Consolidated text. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

326 VDAR Preambulas 105. apsvērums; Council of Europe (2018), Explanatory Report to the Protocol amending ..

iespējamiem izņēmumiem un ierobežojumiem, ievērojot noteiktus nosacījumus, piemēram, neatkarīgu un efektīvu pārskatīšanu un uzraudzību.

Latvijai ir saistošas datu aizsardzības prasības, kas noteiktas starptautiskā līmenī. 2001. gadā Latvija ratificēja Konvenciju 108, pieņemot likumu "Par Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi".[327] 2018. gada 10. oktobrī Latvija parakstīja jauno protokolu un kļuva par vienu no valstīm, kas ir pievienojusies Konvencijai 108+.[328]

Līdzās Konvencijai Eiropas Padome ir pieņēmusi rekomendācijas, rezolūcijas un cita veida dokumentus, kas skaidro Konvencijā noteikto principu interpretāciju un piemērošanu dažādās jomās.[329] Tāpat Eiropas Padome ir pieņēmusi nozīmīgus dokumentus, lai vērstu uzmanību uz masveida novērošanas radīto apdraudējumu cilvēktiesībām. 2015. gadā Eiropas Padomes Ministru komiteja pieņēma Rezolūciju "Par masveida novērošanu".[330] Tā tika pieņemta kā reakcija uz E. Snoudena atklājumiem, vēršot uzmanību, ka atklātā masveida novērošanas prakse apdraud ECTK noteiktās cilvēktiesības, ieskaitot tiesības uz privātumu (8. pants), informācijas un izteiksmes brīvību (10. pants), tiesības uz taisnīgu tiesu (6. pants) un domu, pārliecības un ticības brīvību (9. pants). Šīs tiesības ir demokrātijas stūrakmeņi, un to pārkāpumi bez atbilstošas tiesas kontroles apdraud arī tiesiskumu.[331] Rezolūcijā Ministru komiteja aicināja ES pabeigt darbu pie Vispārīgās datu aizsardzības regulas, kā arī pieņemt atbilstošu regulējumu datu nodošanai uz trešajām valstīm. Savukārt dalībvalstis tika mudinātas pieņemt atbilstošu tiesisko regulējumu, kas attiektos uz izlūkdienestu darbību, kā arī veicināt lietotājam draudzīgu tādu automātisko datu aizsardzības metožu turpmāku attīstību, kas spēj cīnīties pret masveida novērošanu un citiem interneta drošības draudiem, arī ārpus valsts sektora.[332]

2020. gada septembrī Eiropas Padomes Konvencijas 108 Konsultatīvās komitejas priekšsēdētāja Alesandra Pjeruči (*Alessandra Pierucci*) un Eiropas Padomes Datu aizsardzības komisārs Žans Filips Valters (*Jean-Philippe Walter*) pieņēma kopīgu paziņojumu, kurā valstis ir mudinātas stiprināt personas datu aizsardzību

327 Latvijā likums par Konvencijas 108 ratificēšanu pieņemts 2001. gada 5. aprīlī. Sk. Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi.

328 Sk. valstis, kas ir pievienojušās Konvencijai 108+: Council of Europe. Chart of signatures and ratifications of Treaty 223. Status as of 12/06/2021. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures?p_auth=iyy2ZbpX

329 Sk. Council of Europe. Recommendations, resolutions and guidelines. https://www.coe.int/en/web/cdcj/recommendations-resolutions-guidelines

330 Parliamentary Assembly of the Council of Europe. (2015). Resolution 2045. Mass surveillance. http://assembly.coe.int/nw/xml/xref/xref-xml2html-en.asp?fileid=21692&lang=en

331 Ibid., para 4.

332 Ibid., para 18, 19.

izlūkdienestu veiktās digitālās novērošanas kontekstā, pievienojoties Eiropas Padomes Konvencija 108+ un veicinot jaunu starptautisku tiesisku standartu izstrādi, lai šajā jomā nodrošinātu demokrātiskus un efektīvus aizsardzības pasākumus. Paziņojumā norādīts, ka valstīm starptautiskā līmenī ir jāvienojas par to, cik lielā mērā izlūkošanas dienestiem ir atļauts veikt novērošanu, kādos apstākļos un kādi aizsardzības pasākumi jāievēro.[333]

Jaunu tiesisko standartu izveide varētu balstīties uz kritērijiem, kurus jau ir izstrādājušas tiesas, tostarp EST.[334] Paziņojumā tiek vērsta uzmanība uz EST sprieduma "Schrems II" nozīmi. Tajā ir secināts, ka ES un ASV līgums jeb t. s. privātuma vairogs nenodrošina pietiekamu aizsardzības līmeni personas datiem, kas no ES pārsūtīti uz ASV, jo ASV valdības pārraudzītajā novērošanas programmā nav pietiekamu cilvēktiesību aizsardzības pasākumu saistībā ar piekļuvi datiem. Paziņojumā ir uzsvērts, ka šis spriedums ietekmē ne tikai datu nosūtīšanu no ES uz ASV, tas dod arī iespēju nostiprināt vispārējo datu aizsardzības sistēmu. Paziņojumā tiek arī atgādināts, ka Konvencijai 108+ ir būtiska nozīme, lai nodrošinātu stabilu juridiski saistošu vienošanos par privātuma un personas datu aizsardzību visā pasaulē, it īpaši attiecībā uz personas datu plūsmu pāri robežām. Tajā pašā laikā tiek arī norādīts – lai gan Konvencija 108+ paredz stabilu starptautisko tiesisko regulējumu personas datu aizsardzībai, tā pilnībā neatrisina dažādas problēmas, ko digitālajā laikmetā rada bezprecedenta novērošanas iespējas.

Eiropas Padome ir aktīvi iesaistījusies diskusijā un izstrādājusi dokumentus arī par jauno tehnoloģiju, īpaši mākslīgā intelekta sistēmu, ietekmi uz cilvēktiesībām. 2017. gadā Eiropas Padomes Parlamentārā asambleja publicēja Rekomendāciju par tehnoloģiju saplūšanu, mākslīgo intelektu un cilvēktiesībām.[335] Rekomendācijā norādīts, ka nanotehnoloģijas, biotehnoloģijas, informācijas tehnoloģijas un kognitīvo zinātņu saplūšana un ātrums, ar kādu jaunās tehnoloģijas tiek laistas tirgū, ietekmē ne tikai cilvēktiesības un veidu, kā tās var tikt īstenotas, bet arī pamatkoncepciju par to, kas raksturo cilvēku. Jauno tehnoloģiju un to izmantošanas veidu pieaugums izjauc robežas starp cilvēku un mašīnu, starp

333 Council of Europe. (2020). Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. https://rm.coe.int/covid19-joint-statement/16809e09f4

334 Council of Europe. (2020). Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services. Joint statement by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb

335 Parliamentary Assembly of the Council of Europe. (2017). Recommendation 2102. Technological convergence, artificial intelligence and human rights. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en

darbībām tiešsaistē un bezsaistē, starp fizisko un virtuālo pasauli, starp dabisko un mākslīgo. Lai aizsargātu cilvēka cieņu 21. gadsimtā, ir nepieciešamas jaunas pārvaldības formas, publiskas diskusijas un tiesiskie mehānismi. Rekomendācijā Eiropas Padome tiek aicināta attiecīgajām institūcijām uzdot izvērtēt, kā tehnoloģiju saplūšana un tās sociālās un ētiskās sekas, kas saistītas ar ģenētiku un genomiku, neirozinātni un lielo datu jomu, izaicina dažādas cilvēktiesību dimensijas.

Konvencijas 108 Konsultatīvā komiteja ir izstrādājusi vairākus dokumentus, kuros analizēti izaicinājumi, ko jaunās tehnoloģijas, īpaši mākslīgais intelekts, rada cilvēktiesībām. 2017. gadā tika pieņemtas Vadlīnijas par personu aizsardzību attiecībā uz personas datu apstrādi lielo datu pasaulē.[336] 2019. gadā tā publicēja Alesandro Mantelero (*Alessandro Mantelero*) izstrādāto ziņojumu "Mākslīgais intelekts un datu aizsardzība: izaicinājumi un iespējamie aizsardzības līdzekļi".[337] 2019. gadā Konvencijas 108 Konsultatīvā komiteja publicēja Vadlīnijas par mākslīgo intelektu un datu aizsardzību.[338]

2019. gadā Eiropas Padomes Ministru komiteja pieņēma Deklarāciju par algoritmisko procesu manipulācijas iespējām, kas brīdina, ka algoritmiskos procesus var izmantot, lai manipulētu ar sociālo un politisko uzvedību. Deklarācijā tiek vērsta uzmanība uz "draudiem demokrātiskai sabiedrībai", ko rada "mašīnmācīšanās rīku spēja ietekmēt emocijas un domas, kā arī valstis tiek mudinātas šos draudus novērst".[339]

2020. gadā Eiropas Padomes Ministru komiteja pieņēma Rekomendāciju dalībvalstīm par algoritmisko sistēmu ietekmi uz cilvēktiesībām.[340] Tā uzsver, ka cilvēka cieņas aizsardzība un cilvēktiesību un pamatbrīvību aizsardzība, īpaši tiesības uz personas datu aizsardzību, ir būtiskas, izstrādājot un ieviešot mākslīgā intelekta sistēmas, kas var ietekmēt indivīdus un sabiedrību, īpaši, ja šīs sistēmas tiek izmantotas lēmumu pieņemšanas procesos. Vadlīnijās ir norādīts, ka mākslīgā intelekta izstrādei, kas ietver personas datu apstrādi, ir jābalstās uz Konvencijā 108+ noteiktajiem principiem. Šie galvenie principi ir likumība, taisnīgums,

336 Council of Europe (2017), Consultative Committee of the Convention for the Protection .. (T-PD).

337 Council of Europe. (2019). Report on Artificial Intelligence and Data Protection: Challenges and Possible Remedies. https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6

338 Council of Europe. (2019). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). Guidelines of Artificial Intelligence and Data Protection. https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

339 Council of Europe (2019), Declaration by the Committee of Ministers on the manipulative capabilities ..

340 Council of Europe (2020), Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States ..

mērķa precizēšana, datu apstrādes samērīgums, integrēta datu aizsardzība (*privacy by design* – angļu val.) un datu aizsardzība pēc noklusējuma (*privacy by default* – angļu val.), atbildība un atbilstības pierādīšana, pārredzamība, datu drošība un risku pārvaldība. Rekomendācijā tiek uzsvērts, ka uz iespējamām datu apstrādes sekām ir jāskatās plašāk – jāņem vērā ne tikai cilvēktiesības un pamatbrīvības, bet arī ietekme uz demokrātiju un sociālās un ētiskās vērtības.

Eiropas Padomes Ministru komitejas izveidotā CAHAI 2020. gada decembrī publicēja priekšizpētes pētījumu, kurā ir piedāvāti vairāki iespējamie varianti Eiropas tiesiskajam regulējumam.[341] Viena no iespējām būtu spēkā esošo juridiski saistošo tiesisko instrumentu modernizācija, piemēram, pieņemot ECTK papildu protokolu, modernizējot Budapeštas konvenciju par kibernoziegumiem[342] vai Konvenciju 108+. Otra iespēja ir pieņemt jaunu saistošu tiesisko instrumentu, piemēram, konvenciju vai pamatkonvenciju. Pamatkonvencija paredzētu, ka valstis savstarpēji vienotos par tiesiskā regulējuma darbības jomu un procedūru, kas jāievēro, lai piedāvātu efektīvus aizsardzības pasākumus mākslīgā intelekta sistēmām, pamatojoties uz Eiropas Padomes standartiem. Trešā iespēja būtu pieņemt nesaistošus tiesiskus instrumentus. CAHAI vērš uzmanību, ka tiesiskais regulējums, visticamāk, būtu jāveido, apvienojot gan saistošus, gan nesaistošus juridiskus instrumentus, kas cits citu papildinātu. Saistošs horizontāls instruments, t. i., konvencija vai pamatkonvencija, varētu konsolidēt vispārīgus principus, lai novērstu riskus, kas raksturīgi mākslīgā intelekta videi, un iekļautu konkrētākus noteikumus, lai aizsargātu cilvēka cieņu, novērstu kaitējumu un veicinātu cilvēktiesības, demokrātiju, tiesiskumu, kā arī nodrošinātu citas tiesības, ētikas principus un pienākumus – cilvēka brīvību un autonomiju, nediskrimināciju, dzimumu līdztiesību, taisnīgumu un daudzveidību, pārredzamību un izskaidrojamību, datu aizsardzību, tiesības uz privātumu un atbildību. Tas varētu veidot pamatu attiecīgajiem valstu tiesību aktiem šajā jomā un veicināt paraugpraksi mākslīgā intelekta regulējuma izstrādē. Šo instrumentu, kas varētu ietvert atbilstošus pēcpārbaudes mehānismus un procesus, varētu papildināt gan juridiski saistoši, gan nesaistoši Eiropas Padomes instrumenti konkrētās nozarēs, un tie varētu paredzēt turpmākus nozarei specifiskus principus un sīki izstrādātas prasības par to, kā risināt mākslīgā intelekta nozares problēmas.

2021. gada 21. janvārī Eiropas Padome publicēja Vadlīnijas par sejas atpazīšanu, un šajā dokumentā valstis tiek mudinātas izstrādāt un pieņemt speciālus noteikumus, kas regulētu tiesībaizsardzības nolūkos veiktu biometrisko datu

341 Council of Europe, CAHAI (2020), Feasibility Study.

342 Konvencija par kibernoziegumiem. Pieņemta 23.11.2001. (EP, Latvijā spēkā no 01.06.2007.). *Latvijas Vēstnesis,* 26.10.2001., Nr. 171.

apstrādi, izmantojot sejas atpazīšanas tehnoloģijas, kā arī aizliegtu konkrētus šīs tehnoloģijas izmantošanas gadījumus.[343]

Eiropas Padome nebūt nav vienīgā organizācija, kas aktīvi meklē veidus, kā regulēt mākslīgo intelektu. Arī citas organizācijas, kas aplūkotas turpinājumā, aktīvi darbojas, lai ietekmētu datu aizsardzības tiesību, kā arī jauno tehnoloģiju regulējuma attīstību.

4.1.2. OECD

Līdzās Eiropas Padomei, kas datu aizsardzību pamatā skata no cilvēktiesību aizsardzības skatpunkta, Ekonomiskās sadarbības un attīstības organizācija (*Organisation for Economic Cooperation and Development*, OECD – angļu val.) ir izstrādājusi nozīmīgu instrumentu, kas ietekmējis mūsdienu datu aizsardzības tiesību izveidi, bet iezīmē ekonomisko pieeju datu aizsardzībai, – Vadlīnijas par privātuma aizsardzību un pārrobežu personas datu plūsmu.[344]

OECD ir 1961. gadā dibināta starpvaldību organizācija, kuras uzdevums ir veicināt demokrātiju un tirgus ekonomikas principu ievērošanu, kā arī sekmēt valstu ilgtspējīgas tautsaimniecības attīstību globalizācijas kontekstā. Tā apvieno 38 attīstītākās pasaules valstis, sākot no Ziemeļamerikas un Dienvidamerikas līdz Eiropai un Āzijas un Klusā okeāna reģionam, tai skaitā ES dalībvalstis. Latvija par OECD dalībvalsti kļuva 2016. gadā.

OECD pirmām kārtām ir ekonomikas organizācija, un, kā jau liecina tās nosaukums, tās darbība galvenokārt ir saistīta ar sadarbības veicināšanu starp valstīm, lai veicinātu ekonomisko attīstību, finansiālo stabilitāti, dzīves līmeņa paaugstināšanu un starptautiskās tirdzniecības attīstību. Tā koordinē nacionālo un starptautisko politiku izstrādi, tostarp izstrādā vadlīnijas, standartus un starptautiskos tiesību instrumentus galvenokārt ar ekonomiku saistītos jautājumos.

Lai gan OECD darbība atšķirībā no Eiropas Padomes nav primāri saistīta ar cilvēktiesību aizsardzību, tā aktīvi iesaistās datu aizsardzības jautājumu attīstībā. OECD darbs pie privātuma un datu aizsardzības jautājumiem sākās 1969. gadā, kad tika nozīmēta ekspertu grupa, lai analizētu dažādus privātuma jautājumus, tostarp saistībā ar digitālo informāciju, valsts pārvaldi un pārrobežu datu nodošanu. 1979. gadā OECD sarīkoja simpoziju par pārrobežu datu plūsmas un privātuma aizsardzības jautājumiem, tajā piedalījās pārstāvji no dalībvalstīm, privātā sektora un starptautiskām organizācijām. Francijas pārstāvis Luijs Žoinē (*Louis*

343 Council of Europe (2021), .. Convention 108.

344 OECD. (1980). Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Joinet), kurš vēlāk piedalījās vadlīniju izstrādē, uzsvēra ekonomisko vērtību un nacionālo interešu sadursmi, ko rada pārrobežu datu plūsma: "Informācija ir vara, un ekonomiskā informācija ir ekonomiska vara. Informācijai ir ekonomiska vērtība, un spēja uzglabāt un apstrādāt noteikta veida datus vienai valstij var dot politiskas un tehnoloģiskas priekšrocības salīdzinājumā ar citām valstīm."[345]

1978. gadā OECD izveidoja jaunu darba grupu pārrobežu datu barjeru un privātuma aizsardzības jautājumos un tai uzticēja izstrādāt vadlīniju projektu. Darba grupas izstrādātās Vadlīnijas par privātuma aizsardzību un pārrobežu personas datu plūsmu 1980. gadā pieņēma OECD Padome. Vadlīniju mērķis bija saskaņot valstu tiesību aktus, uzsvaru liekot uz šķēršļu novēršanu brīvai datu plūsmai. Vadlīnijās uzsvērts, ka ir jānodrošina, lai privātuma aizsardzības intereses tiktu līdzsvarotas ar personu datu brīvu pārrobežu plūsmu interesēm un nav pieļaujama tādu šķēršļu radīšana personas datu plūsmām, kuri tiek pamatoti ar privātās dzīves un indivīdu brīvību aizsardzību, bet patiesībā ir pieņemti, lai sasniegtu cita veida ierobežojošus mērķus, kuri netiek atklāti paziņoti.[346]

OECD vadlīnijas tika izstrādātas ciešā sadarbībā ar Eiropas Kopienu un Eiropas Padomi, tādējādi nodrošinot to atbilstību datu aizsardzības principiem, kas tajā pašā laikā tika izstrādāti Eiropā. Vadlīnijas tika pārskatītas 2013. gadā. Lai gan vadlīnijas nav juridiski saistošas, tomēr tām bija būtiska nozīme datu aizsardzības tiesību harmonizācijā visā pasaulē.

OECD aktīvi darbojas arī mākslīgā intelekta politikas jomā. 2019. gadā OECD dalībvalstis pieņēma "Padomes Rekomendāciju par mākslīgo intelektu", ko parakstīja 42 valstu pārstāvji un kas nosaka pirmos starptautiskos standartus, par kuriem valdības ir vienojušās, lai izveidotu atbildīgu un uzticamu mākslīgo intelektu.[347] Rekomendācijas mērķis ir sekmēt inovācijas un veicināt uzticamu un atbildīgu mākslīgā intelekta pārvaldību, vienlaikus nodrošinot cilvēktiesību un demokrātisko vērtību ievērošanu.

Rekomendācijā ir noteikti pieci uz vērtībām balstīti principi uzticama mākslīgā intelekta atbildīgai pārvaldībai. Pirmais princips paredz, ka mākslīgajam intelektam vajadzētu dot labumu cilvēkiem un planētai, veicinot iekļaujošu izaugsmi, ilgtspējīgu attīstību un labklājību. Otrais princips – uz cilvēku vērstas vērtības un taisnīgums – paredz, ka mākslīgā intelekta sistēmas būtu jāveido tā, lai tiktu ievērots tiesiskums, cilvēktiesības, demokrātiskās vērtības. Tās ietver brīvību, cieņu un autonomiju, privātumu un datu aizsardzību, nediskrimināciju un vienlīdzību, daudzveidību, taisnīgumu, sociālo taisnīgumu un starptautiski

345 OECD. (2013). The OECD Privacy Framework. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

346 OECD (1980), Recommendation of the Council concerning Guidelines Governing ..

347 OECD (2019), Recommendation of the Council on Artificial Intelligence.

atzītas darba tiesības. Šajā nolūkā būtu jāievieš atbilstoši mehānismi un aizsardzības pasākumi, piemēram, vajadzības gadījumā nodrošinot cilvēka iejaukšanos. Trešais princips paredz, ka ir jābūt pārredzamībai un atbildīgai informācijas atklātībai par mākslīgā intelekta sistēmām, lai nodrošinātu, ka cilvēki saprot sistēmas, ir informēti par to izmantošanu, kā arī tie, kurus ietekmē mākslīgā intelekta sistēmu rezultāti, varētu tos saprast un apstrīdēt. Ceturtais princips paredz, ka mākslīgā intelekta sistēmām visā to dzīves ciklā jādarbojas stabili un droši, iespējamie riski pastāvīgi jānovērtē un jāpārvalda. Pēdējais, piektais, princips nosaka, ka organizācijām un privātpersonām, kas izstrādā, izvērtē vai izmanto mākslīgā intelekta sistēmas, jābūt atbildīgām par to pareizu darbību saskaņā ar iepriekš minētajiem principiem. Rekomendācija sniedz arī piecus vispārējus ieteikumus dalībvalstīm, ko ieviest valstu politikā un starptautiskajā sadarbībā atbildīga mākslīgā intelekta nodrošināšanai, tai skaitā mudinot investēt mākslīgā intelekta pētniecībā un attīstībā un izveidot mākslīgā intelekta normatīvo regulējumu.

2020. gadā OECD izveidoja Mākslīgā intelekta politikas observatoriju jeb novērošanas centru "OECD.AI"[348], kas ir iekļaujošs sabiedriskās politikas centrs mākslīgā intelekta jomā. Tā mērķis ir palīdzēt valstīm izveidot, attīstīt un uzraudzīt uzticamu un atbildīgu mākslīgā intelekta sistēmu attīstību sabiedrības labā. "OECD.AI" ir tiešsaistes platforma, kur mākslīgā intelekta dalībnieki var dalīties ar informāciju un sadarboties, veidojot ar mākslīgo intelektu saistītu politiku. 2020. gadā tika arī nodibināta Globālā mākslīgā intelekta partnerība[349], kuras sekretariāts ir OECD. Tās mērķis ir pārvarēt plaisu starp teoriju un praksi mākslīgā intelekta politikas jomā un nodrošināt mākslīgā intelekta atbildīgu izmantošanu.

4.1.3. ANO, UNESCO un citi globālie standarti

Tiesības uz privātumu ir noteiktas starptautiskos cilvēktiesību aizsardzības līgumos – Vispārējās cilvēktiesību deklarācijas 12. pantā, SPPPT 17. pantā u. c. Savukārt tiesības uz datu aizsardzību vismaz pagaidām nav atzītas par universālām cilvēktiesībām. Globālā līmenī nav panākta vienošanās par juridiski saistošiem minimālajiem datu aizsardzības standartiem, lai gan šādi priekšlikumi ir bijuši. Vienoties par kopīgiem standartiem traucē būtiski atšķirīga pieeja dažādās tiesību

348 Sk. OECD. AI Policy Observatory. https://oecd.ai

349 Globālās mākslīgā intelekta partnerības dibinātāji ir ES, Austrālija, Kanāda, Francija, Vācija, Indija, Itālija, Japāna, Koreja, Meksika, Jaunzēlande, Singapūra, Slovēnija, Lielbritānija un ASV, un tā apvieno nozares, valdības, pilsoniskās sabiedrības un akadēmisko aprindu ekspertus, lai veiktu mākslīgā intelekta pētījumus. Sk. The Global Partnership on Artificial Intelligence. https://gpai.ai

sistēmās, īpaši starp valstīm, kurās tās vēsturiski ir attīstījušās kā cilvēktiesības, un valstīm, kur datu aizsardzībai ir vairāk ekonomisks pamats.[350]

Tajā pašā laikā ANO ir ļoti nozīmīga loma privātuma un datu aizsardzības veicināšanā. 1990. gadā ANO Ģenerālā asambleja publicēja Vadlīnijas datorizētu personas datu failu regulēšanai. Tās paredz principus, kuri kā minimālās prasības valstīm būtu jāietver nacionālajā likumdošanā, piemēram, likumīgums, taisnīgums, precizitāte, noteikts mērķis, ieinteresēto personu piekļuve, nediskriminācijas princips. Kā atsevišķs princips ir paredzēta arī spēja izdarīt izņēmumus no iepriekš minētajiem principiem, ja tie ir nepieciešami, lai aizsargātu valsts drošību, sabiedrisko kārtību un sabiedrības veselību, ja šāda atkāpšanās ir skaidri noteikta likumā vai līdzvērtīgā regulējumā, kas pieņemts saskaņā ar nacionālo tiesību sistēmu, kurā paredzētas skaidras robežas un atbilstoši aizsardzības pasākumi.

Vadlīnijas ietver arī drošības principu, kas nosaka, ka būtu jāveic atbilstoši pasākumi, lai aizsargātu datus no dažāda veida riskiem, piemēram, nejaušas nozaudēšanas vai iznīcināšanas, neatļautas piekļuves, krāpnieciskas datu ļaunprātīgas izmantošanas vai datorvīrusu piesārņojuma. Tās paredz, ka katras valsts likumi nosaka iestādi, kas saskaņā ar tās nacionālo tiesību sistēmu ir atbildīga par iepriekš izklāstīto principu ievērošanas uzraudzību, kā arī paredz pienākumu nodrošināt brīvu datu plūsmu.[351]

ANO ir arī plaši vērsusi uzmanību uz masveida novērošanas radīto apdraudējumu cilvēktiesībām. Reaģējot uz E. Snoudena atklājumiem, 2013. gadā ANO Ģenerālā asambleja pieņēma rezolūciju 68/167 "Tiesības uz privātumu digitālajā laikmetā"[352], kurā pauda bažas par komunikāciju uzraudzības un pārtveršanas, kā arī personas datu vākšanas, it īpaši, ja to veic masveidā, negatīvo ietekmi uz cilvēktiesībām, un mudināja valstis izveidot vai uzturēt neatkarīgus un efektīvus uzraudzības mehānismus, kas var nodrošināt novērošanas darbību pārredzamību un atbildību.

Pēc Ģenerālās asamblejas pieprasījuma 2014. gadā ANO Augstā cilvēktiesību komisāra birojs publicēja ziņojumu "Tiesības uz privāto dzīvi digitālajā laikmetā", kurā ir aplūkota tiesību uz privātumu aizsardzība un veicināšana novērošanas kontekstā, kā arī digitālo komunikāciju pārtveršana un personas datu vākšana, tostarp masveidā.[353] Ziņojumā ir uzsvērts, ka masveida novērošana līdzās tiesībām uz privātumu var ietekmēt arī citas ar tām cieši saistītas tiesības – tiesības uz

350 Lloyd (2020), Information Technology Law, pp. 33, 34.

351 UN General Assembly. (1990). Guidelines for the Regulation of Computerized Personal Data Files. https://www.refworld.org/docid/3ddcafaac.html

352 UN General Assembly. (2013). Resolution 68/167. The right to privacy in the digital age. https://digitallibrary.un.org/record/764407/?ln=en

353 OHCHR (2014), The right to privacy in the digital age.

uzskatu un vārda brīvību, tiesības meklēt, saņemt un izplatīt informāciju, mierīgas pulcēšanās un biedrošanās brīvību un tiesības uz ģimenes dzīvi.

Ziņojumā ir norādīts, ka mērķtiecīga digitālās komunikācijas uzraudzība var būt nepieciešams un efektīvs pasākums izlūkdienestiem un tiesībaizsardzības iestādēm, ja tā tiek veikta saskaņā ar starptautiskajiem un nacionālajiem tiesību aktiem. Valdībai ir jāpierāda, ka iejaukšanās ir nepieciešama un proporcionāla adresētajam specifiskajam riskam. Tādējādi masveida vai "liela apjoma" novērošanas programmas var uzskatīt par patvaļīgām, pat ja tām ir leģitīms mērķis un ja tās ir paredzētas tiesiskajā regulējumā. Ziņojumā minēts: nebūtu pieļaujams, ka "pasākumi ir vērsti uz adatu meklēšanu siena kaudzē"; par atbilstošu ir uzskatāms tāds pasākums, kas ņem vērā ietekmi uz "siena kaudzi" salīdzinājumā ar apdraudēto kaitējumu; proti, vai pasākums ir nepieciešams un samērīgs. Līdzās valsts iestāžu atbildībai turpmākajos ziņojumos arvien vairāk uzmanība pievērsta arī privātā sektora atbildībai par cilvēktiesību ievērošanu un aicinājums uzņēmumiem informēt lietotājus par personas datu vākšanu, izmantošanu, koplietošanu un saglabāšanu, kā arī izveidot pārredzamu datu apstrādes politiku.[354]

2015. gadā ANO Cilvēktiesību padome iecēla IT ekspertu profesoru Džozefu Kanataci (*Joseph Cannataci*) par pirmo īpašo referentu jautājumos par tiesībām uz privātumu. Referenta īpašie uzdevumi ietver informācijas vākšanu par valstu praksi un pieredzi saistībā ar privātumu un jauno tehnoloģiju izaicinājumiem, paraugprakses apmaiņu un veicināšanu, kā arī iespējamo šķēršļu noteikšanu. Viņš ir pievērsis pastiprinātu uzmanību digitālo komunikāciju pārtveršanai un personas datu vākšanai, īpaši masveida novērošanas kontekstā. 2017. gada īpašā referenta ikgadējais ziņojums bija veltīts valsts novērošanas darbībām no nacionālā un starptautiskā skatpunkta un sniedza sākotnējos ieteikumus pasākumu aizsardzības garantijām, uzsverot nepieciešamību nodrošināt pārredzamību un pārskatatbildību.[355] Arī turpmākos ikgadējos ziņojumos pastiprināta uzmanība ir vērsta uz cilvēktiesību riskiem, ko rada valstu masveida novērošanas pasākumi.[356]

354 Sk. OHCHR. (2018). The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. https://digitallibrary.un.org/record/777869#record-files-collapse-header

355 UN Special Rapporteur on the right to privacy. (2017). Report of the Special Rapporteur on the right to privacy. https://digitallibrary.un.org/record/3845912

356 UN Special Rapporteur on the right to privacy. (2018). Report of the Special Rapporteur on the right to privacy. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/324/47/PDF/G1832447.pdf?OpenElement; UN Special Rapporteur on the right to privacy. (2019). Right to privacy. Report of the Special Rapporteur on the right to privacy. https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08;%20https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx

ANO īpašā referenta jautājumos par tiesībām uz privātumu 2020. gada ziņojumā atsevišķa nodaļa ir veltīta drošībai un novērošanai, kurā norādīti ieteikumi valstīm un nevalstiskiem dalībniekiem. Tiem ir jāaizsargā digitālo komunikāciju privātums un visu personu tiesības uz privātumu neatkarīgi no viņu dzimuma, veicinot tādus rīkus kā šifrēšana. Tiem vajadzētu nodrošināt, ka tiesību uz privātumu ierobežojumi – tostarp masveida vai mērķtiecīga novērošana, personas datu pieprasījumu vai šifrēšanas, pseidonimizēšanas un anonimizēšanas rīku izmantošanas ierobežojumi – ir balstīti uz katru gadījumu atsevišķi; nediskriminē pēc dzimuma vai citiem faktoriem; ir saprātīgi, nepieciešami un samērīgi, kā to paredz likums; tiem ir leģitīms mērķis, un tos apstiprina tikai tiesa.[357]

ANO aktīvi iesaistās arī starptautiskajās diskusijās par mākslīgā intelekta regulējumu. 2018. gadā Starptautiskā telekomunikāciju savienība ar vairāk nekā 25 ANO aģentūrām Ženēvā rīkoja "AI for Good" samitu, kurā ANO ģenerālsekretārs Antoniu Gutērrešs (*António Guterres*) atzina, ka, ņemot vērā mākslīgā intelekta straujo attīstību, ir jārada jaunas platformas, lai novērstu tā radītos riskus, un uzsvēra vēlmi, lai ANO būtu platforma, kurā dažādas grupas sanāktu kopā, lai apspriestu un vienotos par protokoliem un citiem mehānismiem, kā nodrošināt, ka kibertelpa, internets un mākslīgais intelekts būtu "labā spēks" (*force for good* – angļu val.).[358] 2018. gadā ANO ģenerālsekretārs pieņēma Jauno tehnoloģiju stratēģiju[359], kurā uzsvērts, ka viens no pamatprincipiem ir, ka jaunajām tehnoloģijām jābalstās uz globālām vērtībām, kas noteiktas ANO Hartā[360] un Vispārējā cilvēktiesību deklarācijā.

2020. gada septembrī ANO īpašais referents jautājumos par tiesībām uz privātumu publicēja projektu Datu privātuma vadlīnijām mākslīgā intelekta izstrādei un darbībai. Vadlīnijas paredzēts piemērot mākslīgā intelekta risinājumiem, kas veic datu apstrādi, visos sektoros, tostarp publiskajā un privātajā sektorā. Vadlīnijas nosaka, ka mākslīgā intelekta risinājumu plānošanā un ieviešanā kā obligāti apsverami šādi septiņi galvenie principi: 1) jurisdikcija; 2) likumīgs pamats un

357 UN Special Rapporteur on the right to privacy. (2020). Report of the Special Rapporteur on the right to privacy. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/071/66/PDF/G2007166.pdf?OpenElement

358 UN News. (5 November, 2018). 'Warp speed' technology must be 'force for good' UN chief tells web leaders. https://news.un.org/en/story/2018/11/1024982

359 UN. (2018). UN Secretary-General's Strategy on new technologies. https://www.un.org/en/newtechnologies/images/pdf/SGs-Strategy-on-New-Technologies.pdf

360 Apvienoto Nāciju Organizācijas Statūti. Pieņemti 26.06.1945. (Latvijā spēkā no 17.09.1991.). *Latvijas Vēstnesis*, 29.01.2018., Nr. 20.

nolūka ierobežojums; 3) atbildība; 4) kontrole; 5) pārredzamība un izskaidrojamība; 6) datu subjekta tiesības; 7) drošības pasākumi.[361]

Vadlīniju projektā ir paredzētas būtiskas datu aizsardzības prasības. Likumīga pamata prasība paredz, ka mākslīgā intelekta risinājumiem, ja tie attiecas uz personas datiem, ir jābūt tiesiskam pamatam, jo personas datu apstrāde vienmēr ietekmē datu subjekta tiesības. Saskaņā ar pārredzamības principu mākslīgā intelekta risinājumiem ir jābūt pārredzamiem sabiedrībai un datu subjektiem. Vadlīnijās ir noteiktas datu subjektu tiesības, tostarp: tiesības uz informāciju; tiesības uz samērīgu piekļuvi saviem datiem, kas ietver izsmeļošu rakstisku informāciju par personas datiem un to, kā tie tiek izmantoti un apstrādāti, kā arī sekām un veidiem, kā mākslīgā intelekta sistēmu rezultāti var ietekmēt datu subjekta stāvokli un individuālās tiesības; tiesības pieprasīt cilvēka lēmumu, ja ir pamatotas šaubas par to, vai mākslīgā intelekta risinājuma piedāvātais vai pieņemtais lēmums nav pareizs; tiesības labot datus, ja tie ir nepareizi; tiesības iesniegt sūdzību, ja ir pamatots iemesls.

Daudzas ANO aģentūras, iestādes un pētniecības institūti aktīvi iesaistās atbildīga mākslīgā intelekta veicināšanā. 2019. gadā tika publicēts ANO Starpreģionālās noziedzības un tieslietu pētniecības institūta (UNICRI) un Starptautiskās Kriminālpolicijas organizācijas (Interpol) kopīgs ziņojums par mākslīgo intelektu un robotiku tiesībaizsardzības iestādēs, kurā norādīts, ka mākslīgais intelekts un robotika ievērojami veicinās tiesībaizsardzības iestāžu novērošanas iespējas un tāpēc būs jārisina ar šīm tehnoloģijām saistītās privātuma problēmas.[362]

Konkrētāk uz novērošanas tehnoloģiju riskiem un nepieciešamo regulējumu uzmanību vērsusi ANO Augstā cilvēktiesību komisāra biroja Rasu diskriminācijas izskaušanas komiteja, kas 2020. gadā pieņēma Vispārējo rekomendāciju Nr. 36 par rasu profilēšanas novēršanu un apkarošanu, ko veic tiesībaizsardzības iestāžu amatpersonas.[363] Rekomendācijas 53. punktā ir atzīts, ka sejas atpazīšanas un novērošanas tehnoloģiju aizvien plašāka izmantošana, lai izsekotu un kontrolētu cilvēkus pēc konkrētām demogrāfiskām pazīmēm, rada bažas par daudzām cilvēktiesībām, tostarp tiesībām uz privātumu, mierīgas pulcēšanās un biedrošanās brīvību, vārda brīvību un pārvietošanās brīvību. Šīs tehnoloģijas ir izstrādātas, lai automātiski identificētu personas, pamatojoties uz viņu sejas ģeometriju, kas

361 UN Special Rapporteur on the right to privacy. (2020). Draft for Consultations. Data Privacy Guidelines for the development and operation of Artificial Intelligence solutions. https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2020_Sept_draft_data_Privacy_guidelines.pdf

362 UNICRI & INTERPOL. (2019). Artificial Intelligence and Robotics for Law Enforcement. https://unicri.it/artificial-intelligence-and-robotics-law-enforcement

363 UN Committee on the Elimination of Racial Discrimination. (2020). General recommendation No. 36. Preventing and Combating Racial Profiling by Law Enforcement Officials. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/349/50/PDF/G2034950.pdf?OpenElement

ļauj potenciāli profilēt tās, balstoties uz diskriminējošiem pamatiem, piemēram, rasi, ādas krāsu, nacionālo vai etnisko izcelsmi vai dzimumu. Turklāt ir pierādīts, ka sejas atpazīšanas tehnoloģijas precizitāte var atšķirties atkarībā no novērtēto personu ādas krāsas, etniskās piederības vai dzimuma, un tas var izraisīt diskrimināciju. Tālāk Rekomendācijas 59. punktā ir norādīts, ka, pirms tiek izmantotas sejas atpazīšanas tehnoloģijas, valstīm ir rūpīgi jāizvērtē to ietekme uz cilvēktiesībām, jo tās var izraisīt kļūdainu identifikāciju. Pirms to ieviešanas valstīm būtu jāapsver izmēģinājuma periods, kura laikā šo tehnoloģiju darbību uzraudzītu neatkarīgas institūcijas un šo tehnoloģiju precizitāte tiktu pārbaudīta, iekļaujot personas, kas pārstāv dažādas iedzīvotāju grupas, lai samazinātu iespēju, ka personas tiek nepareizi identificētas un profilētas atkarībā no ādas krāsas.

UNESCO ir pieņēmusi Rekomendāciju par mākslīgā intelekta ētiku.[364] Tā ir pirmā globālā vienošanās, kas nosaka standartus mākslīgā intelekta ētikas jomā. UNESCO ģenerāldirektore Odrē Azulē (*Audrey Azoulay*) 2020. gada martā nozīmēja 24 ekspertus, izveidojot starptautisko *ad hoc* ekspertu grupu (AHEG), kas 2020. gadā sagatavoja pirmo rekomendācijas projektu.[365] 2020. gada vasarā notika plašs tā apspriešanas process. Tā paša gada septembrī Rekomendācijas projekts tika nodots dalībvalstīm. 2021. gadā aprīlī un jūnijā tas tika izskatīts UNESCO Starpvaldību komitejā. 2021. gada 24. novembrī UNESCO Ģenerālās konferences 41. sesijā 193 valstis vienojās par Rekomendācijas par mākslīgā intelekta ētiku pieņemšanu.

Rekomendācijas mērķis ir nodrošināt, lai mākslīgā intelekta sistēmas darbotos cilvēces, personu, sabiedrības, kā arī vides un ekosistēmu labā, kā arī novērst to radīto kaitējumu. Rekomendācijas mērķis ir arī veicināt mākslīgā intelekta sistēmu miermīlīgu izmantošanu (5. punkts). Rekomendācija veicina cilvēktiesību, cilvēka cieņas, dzimumu līdztiesības, tiesiskuma un demokrātijas vērtību ievērošanu. Lai gan tajā īpaša uzmanība pievērsta mākslīgā intelekta sistēmu ietekmei uz UNESCO galvenajām darbības jomām – izglītību, zinātni, kultūru, komunikāciju un informāciju –, tajā pašā laikā tās noteikumi ir vispārīgi un attiecināmi uz ikvienu mākslīgā intelekta jomu.

Rekomendācija ne tikai nosaka vērtības un principus, bet arī sniedz konkrētus ieteikumus un paredz praktiskus to īstenošanas mehānismus. Valstis tiek aicinātas tos ņemt vērā, izstrādājot savus tiesību aktus, politikas dokumentus vai citus instrumentus attiecībā uz mākslīgo intelektu saskaņā ar starptautiskajām tiesībām. Rekomendācija balstās uz četrām vērtībām. Tās ir:

364 UNESCO (2021), Recommendation on the Ethics of Artificial Intelligence.

365 UNESCO. (2020). Composition of the Ad Hoc Expert Group (AHEG) for the Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000372991.

1) cilvēktiesību, pamatbrīvību un cilvēka cieņas ievērošana, aizsardzība un veicināšana;
2) vides un ekosistēmas aizsardzības veicināšana;
3) daudzveidības un iekļaušanas nodrošināšana;
4) dzīvošana mierīgā, taisnīgā un savstarpēji saistītā sabiedrībā.

Ja vērtības motivē, sniedz ideālus un iedvesmo uz rīcību, tad principi konkrētāk definē šīs vērtības, lai tās varētu vieglāk ietvert konkrētos politikas ieteikumos. Rekomendācijā ir noteikti desmit principi: 1) proporcionalitāte un nekaitēšana; 2) drošība; 3) taisnīgums un nediskriminācija; 4) ilgtspējība; 5) tiesības uz privātumu un datu aizsardzība; 6) cilvēka pārraudzība; 7) pārredzamība un izskaidrojamība; 8) atbildība; 9) apzināšanās un zināšanas; 10) daudzpusīga un adaptīva pārvaldība un sadarbība.

Pirmais princips – proporcionalitāte un nekaitēšana – paredz, ka izvēle izmantot mākslīgā intelekta sistēmas un to, kuru mākslīgā intelekta metodi izmantot, būtu jāpamato šādi:

a) izvēlētajai mākslīgā intelekta metodei jābūt piemērotai un samērīgai, lai sasniegtu noteiktu leģitīmu mērķi;
b) izvēlētā mākslīgā intelekta metode nedrīkst pārkāpt rekomendācijā ietvertās pamatvērtības, it īpaši tās izmantošana nedrīkst pārkāpt cilvēktiesības;
c) mākslīgā intelekta metodei jāatbilst kontekstam un jābūt balstītai uz stingriem zinātniskiem pamatiem.

Minētais princips nosaka arī mākslīgā intelekta sistēmu izmantošanas sarkanās līnijas. Tas nosaka, ka gadījumos, kad lēmumiem var būt neatgriezeniska vai grūti maināma ietekme vai tie var ietvert lēmumus par dzīvību un nāvi, galīgais lēmums ir jāpieņem cilvēkam. Tālāk tas paredz, ka mākslīgā intelekta sistēmas nedrīkst izmantot sociālās vērtēšanas vai masveida novērošanas nolūkos (25. punkts).

Rekomendācijā galvenā uzmanība ir veltīta politikas ieteikumiem. Viens no būtiskākajiem ieteikumiem ir, lai dalībvalstis ieviestu efektīvus mehānismus (ieskaitot politikas pamatnostādnes vai mehānismus) un nodrošinātu, ka visas ieinteresētās personas (piemēram, privātā sektora uzņēmumi, akadēmiskās un pētniecības iestādes), kā arī pilsoniskā sabiedrība tos ievēro, cita starpā palīdzot visām ieinteresētajām pusēm izstrādāt cilvēktiesību, tiesiskuma, demokrātijas un ētikas ietekmes novērtējumu un uzticamības pārbaudes rīkus. Šādas politikas vai mehānismu izstrādes procesā būtu jāiekļauj visas ieinteresētās puses, un tajā būtu jāņem vērā katras dalībvalsts apstākļi un prioritātes (49. punkts).

UNESCO var atbalstīt dalībvalstis politikas mehānismu izstrādē, kā arī uzraudzībā un novērtēšanā. Lai varētu efektīvi īstenot rekomendāciju, UNESCO apņemas izstrādāt gatavības novērtēšanas metodiku, lai palīdzētu dalībvalstīm noteikt savu statusu, ņemot vērā, ka valstis var atrasties dažādās stadijās

attiecībā uz gatavību ieviest Rekomendāciju dažādās jomās, piemēram, zinātniskajā, tehnoloģiju, ekonomiskajā, izglītības, juridiskajā, regulatīvajā, infrastruktūras, sabiedrības, kultūras jomā. Tāpat UNESCO apņemas atbalstīt dalībvalstis mākslīgā intelekta tehnoloģiju ētiskās ietekmes novērtēšanas metodikas izstrādē (49. punkts).

Rekomendācijā ietvertas vienpadsmit politikas plānošanas jomas: ētiskās ietekmes novērtējums; ētiska pārvaldība; datu politika; starptautiskā sadarbība un attīstība; vide un ekosistēmas; dzimumu līdztiesība; kultūra; izglītība un zinātne; komunikācija un informācija; ekonomika un darbaspēks; veselība un labklājība.

Viens no būtiskākajiem rekomendācijā paredzētajiem mehānismiem ir ētiskās ietekmes novērtējums. Dalībvalstis tiek aicinātas ieviest šādus novērtējumus, kas ļautu noteikt mākslīgā intelekta sistēmu ieguvumus, bažas un riskus, kā arī to novēršanas, mazināšanas un uzraudzības pasākumus. Ir nepieciešams novērtēt mākslīgā intelekta plašāku ietekmi uz cilvēktiesībām, darba tiesībām, vidi un ekosistēmu, kā arī ētisko un sociālo ietekmi (50. punkts).

Ētikas pārvaldības politikas joma paredz arī, ka dalībvalstīm būtu jānodrošina, lai mākslīgā intelekta sistēmu radītais kaitējums tiek izmeklēts un atlīdzināts, ieviešot spēcīgus aizsardzības mehānismus un pasākumus atbilstošas atlīdzības nodrošināšanai, lai garantētu cilvēktiesību un pamatbrīvību, un tiesiskuma ievērošanu digitālajā un fiziskajā pasaulē (55. punkts). Tiesiskajam regulējumam, kas attiecas uz mākslīgā intelekta sistēmām, jāatbilst starptautisko cilvēktiesību normām un jāveicina cilvēktiesības un pamatbrīvības visā mākslīgā intelekta sistēmas dzīves cikla laikā (61. punkts). Dalībvalstīm būtu jānosaka skaidras prasības mākslīgā intelekta sistēmas pārredzamībai un izskaidrojamībai, lai palīdzētu nodrošināt tās uzticamību (70. punkts).

Datu politikas joma paredz, ka dalībvalstīm ir jāievieš atbilstošas aizsardzības garantijas, lai atzītu un aizsargātu personas pamattiesības uz privātumu, tostarp pieņemot vai īstenojot tiesisko regulējumu, kas nodrošina atbilstošu aizsardzību un atbilst starptautiskajiem tiesību aktiem (72. punkts). Tām būtu arī jānodrošina, ka personas saglabā tiesības uz saviem personas datiem un tos aizsargā regulējums, kas it īpaši paredz pārredzamību, piemērotus drošības pasākumus sensitīvu datu apstrādei, augstāko datu drošības līmeni, efektīvas un jēgpilnas atbildības shēmas un mehānismus, pilnīgu datu subjektu tiesību izmantošanu (73. punkts).

Rekomendācija īpaši uzsver nepieciešamību izstrādāt atbilstošu tiesisko regulējumu, kā arī praktiskus to īstenošanas mehānismus. Lai gan ētikas standartiem ir būtiska loma risku novēršanā un samazināšanā, tajā pašā laikā ir svarīgi arī domāt, kā praksē īstenot šos ētikas principus. Kā atzīst Oksfordas Universitātes Interneta institūta pētnieks Brents Mitelštats (*Brent Mittelstadt*), bez būtiskām izmaiņām regulējumā principu ieviešana praksē paliks konkurējošs,

nevis sadarbības process.[366] Tiesiskās prasības ir svarīgs instruments, lai panāktu atbildību un nodrošinātu ētikas principu un sociālo vērtību īstenošanu praksē. Tāpēc ir pilnībā jāizvērtē esošā tiesiskā regulējuma atbilstība un nepilnības, un nepieciešamība pieņemt jaunu regulējumu.

Vienoties par globālu regulējumu traucē atšķirīgā izpratne par dažādiem principiem un to piemērošanu praksē, par to, kā samērojamas konkurējošas intereses, tostarp par privātuma un datu aizsardzības prasībām.[367] ES cilvēktiesību un datu aizsardzības augstie standarti bieži vien noder par paraugu citām valstīm un ietekmē arī mākslīgā intelekta starptautisko regulējumu.

4.2. Eiropas Savienība: no datu aizsardzības zelta standartiem līdz mākslīgā intelekta regulējumam

4.2.1. No ekonomiskās līdz cilvēktiesībās balstītai pieejai

ES sākotnēji tika veidota kā ekonomikas kopiena, nevis organizācija, kas aizsargā cilvēktiesības. Tajā pašā laikā pakāpeniski cilvēktiesību ievērošana ES ieguva arvien būtiskāku nozīmi, un mūsdienās ES ir kļuvusi par spilgtu piemēru uz cilvēktiesībām balstītai pieejai datu aizsardzībai.

ES datu aizsardzības regulējums sāka attīstīties, lai harmonizētu dalībvalstu datu aizsardzības režīmus un tādējādi nodrošinātu vienotu personas datu aizsardzības līmeni un brīvu datu plūsmu starp ES dalībvalstīm. Atšķirīgs tiesiskais regulējums datu aizsardzības jomā rada draudus ekonomiskajai darbībai un brīvai konkurencei ES iekšējā tirgū, kas balstās uz brīvu datu plūsmu starp dalībvalstīm. Lai novērstu šķēršļus brīvai personas datu plūsmai ES un nepieļautu, ka valstis to nepamatoti ierobežo, atsaucoties uz nepieciešamību aizsargāt personu tiesības un brīvības, īpaši tiesības uz privātumu, bija svarīgi nodrošināt vienādu pamattiesību aizsardzības līmeni visās dalībvalstīs.

1992. gada Līgumā par Eiropas Savienību pamattiesību ievērošanas princips tika atzīts par ES vispārējo tiesību principu, kā arī noteikts, ka ES respektē pamattiesības atbilstoši ECTK un dalībvalstu kopīgām konstitucionālām tradīcijām (6. pants).[368]

1995. gada 24. oktobrī Eiropas Parlaments un Padome pieņēma Direktīvu 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu

366 Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1, pp. 501–507. https://doi.org/10.1038/s42256-019-0114-4

367 Jobin, A., Ienca, M., Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, pp. 389–399. https://doi.org/10.1038/s42256-019-0088-2

368 Līgums par Eiropas Savienību, 1992. *OV C* 325, 24.12.2002.

datu brīvu apriti (Direktīva 95/46/EK).[369] Tā bija galvenais ES tiesību akts datu aizsardzības jomā līdz 2018. gadam, kad sāka piemērot VDAR. Direktīva 95/46/EK ieviesa detalizētus personas datu aizsardzības noteikumus un uzraudzības mehānismu. Tajā tika noteikti personas datu apstrādes principi, datu subjektu tiesības, pienākums garantēt datu apstrādes konfidencialitāti un drošību, kā arī noteikumi personas datu pārsūtīšanai uz trešajām valstīm. Direktīva 95/46/EK paredzēja pienākumu dalībvalstīm nodrošināt tiesiskās aizsardzības līdzekļus, sankcijas un atbildību personas datu aizsardzības pārkāpumu gadījumā. Tā uzlika pienākumu katrai dalībvalstij izveidot neatkarīgu datu aizsardzības iestādi. Tā arī ieviesa uzraudzības mehānismu – paziņošanas pienākumu, kā arī personas datu apstrādes reģistrēšanu, kuru VDAR vairs neparedz. Tika izveidota padomdevēja iestāde – Darba grupa personu aizsardzībai attiecībā uz personas datu apstrādi – jeb tā sauktā 29. panta darba grupa, kas pieņēma vadlīnijas par dažādiem personas datu aizsardzības jautājumiem. Daudzas no šīm vadlīnijām apstiprināja Eiropas Datu aizsardzības kolēģija, kas tika izveidota 29. panta darba grupas vietā līdz ar VDAR spēkā stāšanos.

Latvijā datu aizsardzības tiesības sākotnēji attīstījās, pārņemot ES tiesisko regulējumu. Lai ieviestu Direktīvu 95/46/EK, 2000. gada 6. aprīlī tika pieņemts Fizisko personu datu aizsardzības likums. Pamatojoties uz minēto likumu, tika izveidota Datu valsts inspekcija. Likums bija spēkā līdz pat 2018. gadam, kad tika uzsākta VDAR piemērošana.

Dalībvalstīm lielākoties paredzēta rīcības brīvība attiecībā uz veidu, kādā direktīvas normas pārņemt nacionālajā tiesību sistēmā. Tādējādi Direktīva 95/46/EK nenodrošināja pietiekamu datu aizsardzības regulējuma harmonizāciju. ES dalībvalstu datu aizsardzības likumi, kas tika pieņemti, lai ieviestu Direktīvu 95/46/EK, paredzēja būtiski atšķirīgus noteikumus, kā arī datu aizsardzības prakse dažādās dalībvalstīs bija atšķirīga, piemēram, attiecībā uz sodu piemērošanu, kā arī kārtību, kādā uzņēmējiem jāinformē dalībvalstis par veikto datu apstrādi.

Būtisks solis pamattiesību, to skaitā tiesību uz datu aizsardzību, attīstībā bija Hartas pieņemšana 2000. gadā, kas iezīmē pāreju no ekonomiskās uz cilvēktiesību pieeju datu aizsardzībai.

4.2.2. Tiesības uz datu aizsardzību kā atsevišķas pamattiesības

Hartā ir izmantota atšķirīga pieeja no ECTK un citiem agrāk pieņemtiem starptautiskiem cilvēktiesību dokumentiem, nosakot tiesības uz personas datu aizsardzību kā atsevišķas patstāvīgas cilvēka pamattiesības, kas ir nošķiramas no

369 Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti. *OV L* 281, 23.11.1995.

tiesībām uz privāto dzīvi. Tiesības uz privātās dzīves neaizskaramību ir noteiktas Hartas 7. pantā, bet tiesības uz personas datu aizsardzību – 8. pantā.

Hartas 8. panta 1. punktā ir vispārīgi atrunātas ikvienas personas tiesības uz savu personas datu aizsardzību, savukārt otrā daļa paredz piecas un trešā daļa vēl vienu prasību, kas ir atrodamas pirms tam pieņemtajā Direktīvā 95/46/EK, kā arī dalībvalstu datu aizsardzības tiesību aktos. Hartas 8. panta 2. punkts paredz, ka personas dati ir "jāapstrādā godprātīgi, noteiktiem mērķiem un ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos. Ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos." Savukārt 8. panta 3. punkts nosaka, ka atbilstību iepriekš minētajiem datu aizsardzības noteikumiem kontrolē neatkarīga iestāde.

ES datu aizsardzības regulējuma attīstībā izšķiroša nozīme bija Lisabonas līgumam, kas stājās spēkā 2009. gada 1. decembrī. Līdz ar Lisabonas līgumu Harta ieguva juridiski saistošu spēku. Tiesību uz datu aizsardzību kā atsevišķu pamattiesību noteikšana Hartā, kas ir primārais ES tiesību akts, liecina par ES pāreju no ekonomiskās pieejas datu aizsardzībā uz pamattiesībās balstītu pieeju.[370]

Tiesību uz datu aizsardzību kā atsevišķu pamattiesību atzīšana ES lielā mērā atbilst starptautisko cilvēktiesību zinātnieku atzītiem kritērijiem, lai tiktu ieviestas jaunas cilvēktiesības:

1) datu aizsardzība atspoguļo sociālas pamatvērtības straujajā jauno tehnoloģiju attīstības laikmetā;
2) tām zināmu laiku bijusi svarīga nozīme nacionālās, starptautiskās un starpvalstu sistēmās;
3) tās ir atbilstošas spēkā esošajam tiesību aktu kopumam nozarē;
4) ar tām tiek panākta augsta līmeņa vienošanās, vismaz ES;
5) tās rada jaunas tiesības un pienākumus.[371]

Akadēmiskajā literatūrā tiek norādīti vairāki iespējamie iemesli, kāpēc tiesības uz datu aizsardzību tika atzītas par atsevišķām pamattiesībām. Tiek norādīts, ka ES ir attīstījusies vairāk kā ekonomiska savienība, kur datu aizsardzība kā pamattiesības ir piemērojamas ne tikai attiecībā uz datu apstrādi, kas notiek komerciālos nolūkos kopējā tirgus ietvaros, lai aizsargātu iekšējo tirgu, bet tās ir kļuvušas par tiesisku prasību visā ES, tai skaitā arī attiecībā uz apstrādi tiesībaizsardzības nolūkos. Tāpat tiek atgādināts, ka tiesības uz datu aizsardzību aizsargā vērtības, kas "iziet ārpus" privātuma. Turklāt šādā veidā tiek atzītas konstitucionālās tradīcijas, kas pastāv dažās ES valstīs, piemēram, Francijā un Vācijā, kur tiesības uz datu aizsardzību netiek skatītas saistībā ar privātumu. Visbeidzot, kā pamatojums tiek minēts, ka saskaņā ar pragmatisko pieeju tiesības uz datu

370 Sk. Tzanou (2019), *The Fundamental Right to Data Protection*, p. 18.

371 Ibid., p. 20.

aizsardzību ļauj indivīdiem apzināties un izmantot savas tiesības, saskaroties ar jaunajiem izaicinājumiem, ko rada straujā tehnoloģiju attīstība.[372]

Tiesības uz datu aizsardzību un tiesības uz privātumu ir savā starpā cieši saistītas, tomēr patstāvīgas pamattiesības.[373] Rodas jautājums, kā minētās tiesības ir nodalāmas un atšķiras viena no otras.

Datu aizsardzība tiek uzskatīta par jaunākām, modernām un aktīvām tiesībām. Jebkurai personiskās informācijas jeb datu apstrādei jāatbilst datu aizsardzības pamatprasībām, piemēram, ir jāievēro noteiktas personu tiesības.[374] Tiesības uz personas datu aizsardzību stājas spēkā, kad tiek apstrādāti personas dati neatkarīgi no tā, kā tas ietekmē privātumu. Tādējādi tās ir plašākas par tiesībām uz privāto dzīvi. Ne visa datu apstrāde var radīt privātuma aizskārumu.[375]

Līdzīgi kā tiesības uz privātumu, arī tiesības uz datu aizsardzību ir saistītas un palīdz aizsargāt daudzas pamattiesības. Tiesībām uz datu aizsardzību ir būtiska nozīme tiesību uz privātumu nodrošināšanā, turklāt tās aizsargā citas vērtības, piemēram, diskriminācijas aizlieguma principa ievērošanu, paredzot ierobežojumus personu profilēšanai. Vācijā tiesības uz datu aizsardzību izriet no tiesībām uz "informācijas autonomiju". To pamatā savukārt ir tiesības uz "informācijas pašnoteikšanu", kas dod tiesības personai kontrolēt, kāda informācija par viņu tiek atklāta un kā dati tiek izmantoti.[376] Minētās tiesības izriet no cilvēka cieņas principa. Kā atklāts iepriekš, jautājums, cik lielā mērā personām ir tiesības neatklāt informāciju par sevi, ņemot vērā cilvēka cieņas prasību, kļūst arvien aktuālāks līdz ar arvien pieaugošo tendenci izmantot datu apstrādes algoritmus, lai novērotu personas identificējošu informāciju un to izmantotu, lai labāk saprastu, analizētu un paredzētu personu uzvedību.

Tajā pašā laikā tiesības uz datu aizsardzību ir šaurākas nekā tiesības uz privātumu. Privātuma jēdziens ir plašāks, jo tas ietver dažādus privātās sfēras aspektus, piemēram, reputāciju, identitāti, attiecības ar citiem un ārpasauli, fizisko un psiholoģisko integritāti, ģimenes dzīvi, mājas, elektronisko komunikāciju utt.[377] Līdz ar to tiesības uz privātumu un datu aizsardzību ir atšķirīgas tiesības. Turklāt tiek arī norādīts, ka atšķirībā no privātuma, kam ir subjektīvs raksturs, tiesības

372 Sk. Tzanou (2019), *The Fundamental Right to Data Protection*, p. 21.

373 ES Pamattiesību aģentūra, ECT, EP, EDAU (2018), Rokasgrāmata, 18. lpp.

374 Turpat, 19. lpp.

375 Turpat, 18. lpp.

376 Tzanou (2019), *The Fundamental Right to Data Protection*, p. 29.

377 Van Dijk et al. (2018), *Theory and Practice of the European Convention on Human Rights*, p. 669.

uz datu aizsardzību var uzskatīt par "objektīvāka" rakstura tiesībām, ņemot vērā to procesuālo raksturu.[378]

4.2.3. Datu aizsardzības reforma un Vispārīgā datu aizsardzības regula

Ar Lisabonas līgumu tiesības uz datu aizsardzību tika ietvertas Līgumā par Eiropas Savienības darbību (LESD), kā arī tika paplašināta ES kompetence pieņemt tiesību aktus datu aizsardzības jomā. LESD 16. panta 1. punkts paredz ikvienas personas tiesības uz savu personas datu aizsardzību. Tālāk 16. panta 2. punkts nosaka, ka Eiropas Parlaments un Padome paredz noteikumus par fizisko personu aizsardzību attiecībā uz ES iestāžu un struktūru veikto personas datu apstrādi, kā arī personas datu apstrādi, ko veic dalībvalstis saistībā ar ES tiesību aktu darbību, un noteikumus par šādu datu brīvu apriti, un ka šo noteikumu izpildi kontrolē neatkarīgas iestādes.

LESD 16. panta 2. punkts ieviesa jaunu juridisko pamatu ES tiesību aktu pieņemšanai datu aizsardzības jomā. Turklāt ar Lisabonas līgumu brīvības, drošības un tiesiskuma joma tika pielīdzināta pārējām ES jomām, kurās ES ir pilnvaras pieņemt tiesību aktus, kas bija pamatā datu aizsardzības direktīvas izstrādei policijas un tiesu iestāžu sadarbībai krimināltiesību jomā.

Datu aizsardzības tiesiskā regulējuma reforma tika veikta, lai harmonizētu, kā arī modernizētu ES pastāvošo tiesisko regulējumu, ņemot vērā būtiskās izmaiņas, ko bija radījusi informācijas un komunikācijas tehnoloģiju attīstība, jauno tehnoloģiju straujā izplatība un globalizācija kopš Direktīvas 95/46/EK pieņemšanas 1995. gadā. Tāpat bija nepieciešami jauni datu aizsardzības noteikumi, lai cīnītos ar terorisma un noziedzības radītajām problēmām.

Datu aizsardzības reformu Eiropas Komisija ierosināja 2012. gadā, kad tā nāca klajā ar priekšlikumu tiesību aktu paketei, kurā ietilpa VDAR un Policijas direktīva. Pēc ilga likumdošanas procesa abi ES tiesību akti tika pieņemti 2016. gadā un ir piemērojami no 2018. gada maija. Jaunā datu aizsardzības tiesiskā regulējuma pieņemšana ir nozīmīgs solis, lai sasniegtu 2015. gada Digitālā vienotā tirgus stratēģijas[379] mērķus – palielinātu uzticību digitālajiem pakalpojumiem un to drošību.

VDAR, kas piemērojama no 2018. gada 25. maija, aizstāj Direktīvu 95/46/EK un paredz vienotus noteikumus, kuri tieši piemērojami visās ES dalībvalstīs. Tās

378 Tzanou, M. (2013). Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 3(2), https://doi.org/10.1093/idpl/ipt004

379 Eiropas Komisija. (2015). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Digitālā vienotā tirgus stratēģija Eiropai. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex%3A52015DC0192

uzdevums ir stiprināt pamattiesības digitālajā laikmetā, ļaujot fiziskām personām kontrolēt savus personas datus, un vienlaikus nodrošināt brīvu datu plūsmu un ļaut uzņēmējiem maksimāli izmantot digitālā vienotā tirgus sniegtās priekšrocības, mazinot birokrātiju un veicinot patērētāju uzticību.

VDAR ir nostiprināti Direktīvā 95/46/EK noteiktie personas datu aizsardzības principi un datu subjektu tiesības, tās attīstot un papildinot. VDAR piešķir arī ES un dalībvalstīm iespēju tiesību aktos noteikt ierobežojumus datu subjekta tiesību un pienākumu darbībai, to starpā attiecībā uz pārziņa pienākumu ziņot datu subjektam par personas datu aizsardzības pārkāpumiem un personas datu apstrādes principu piemērošanu, ja šādi ierobežojumi ir nepieciešami demokrātiskā sabiedrībā un samērīgi, lai garantētu būtiskus sabiedrības interešu mērķus, piemēram, valsts drošību, aizsardzību, sabiedrisko drošību, vai lai aizstāvētu citu personu tiesības un brīvības (23. panta 1. punkts). Paredzot šādus ierobežojumus, tiesību aktā ir jāietver arī konkrēti noteikumi par datu apstrādi, lai garantētu likumīgu un godprātīgu apstrādi (VDAR 23. panta 2. punkts).

VDAR nosaka vispārīgu pienākumu uzņēmumiem un organizācijām veikt "atbilstošus tehniskus un organizatoriskus pasākumus", lai aizsargātu personas datus, kā arī nosaka konkrētus pasākumus, kas jāveic, lai nodrošinātu atbilstību VDAR, to skaitā reģistrēt apstrādes darbības (30. pants), veikt novērtējumu par šo darbību ietekmi uz datu aizsardzību (35. pants), ieviest atbilstošus drošības pasākumus (32. pants), iecelt datu aizsardzības speciālistu (37. pants), ziņot par datu aizsardzības pārkāpumiem (33. un 34. pants).

Pārzinim[380] ir arī jāīsteno atbilstīga personas datu pārvaldības politika, ciktāl tas ir samērīgi ar apstrādes darbībām. VDAR ir noteikta uz risku balstīta pieeja, kas paredz, ka pasākumi ir jāīsteno, ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūku, kā arī paredz dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām. Tādējādi tie var atšķirties katrā konkrētajā gadījumā, un pašam pārzinim ir jānosaka, kādi pasākumi ir nepieciešami. Šādi pasākumi var būt iekšējo procedūru, piemēram, personas datu aizsardzības politikas, pieņemšana un ieviešana praksē, atbildīgo personu nozīmēšana, regulāras apmācības utt.

Pārzinim ir pienākums kontrolēt personas datus, arī uzticot tos citiem, piemēram, glabāšanai. VDAR nosaka pienākumu pārzinim izmantot tikai tādus apstrādātājus[381], kas sniedz pietiekamas garantijas, ka tiks īstenoti atbilstoši tehniskie

380 VDAR 4. panta 7. punkts nosaka, ka pārzinis ir "fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus".

381 VDAR 4. panta 8. punkts nosaka, ka apstrādātājs ir "fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus".

un organizatoriskie pasākumi tādā veidā, lai apstrādē tiktu ievērotas VDAR prasības un tiktu nodrošināta datu subjekta tiesību aizsardzība (28. panta 1. punkts).

VDAR paredz vairākus būtiskus jaunievedumus. Tā ievieš integrētas datu aizsardzības principu un datu aizsardzības pēc noklusējuma principu, pārredzamības principu un tiesības uz datu pārnesamību. VDAR uzliek pienākumu noteiktos gadījumos veikt novērtējumu par ietekmi uz datu aizsardzību, kā arī nozīmēt datu aizsardzības speciālistu. Vienlaikus tā atceļ iepriekš pastāvošo personas datu apstrādes reģistrēšanu uzraudzības iestādēs. Detalizētāk datu aizsardzības prasības un to piemērošana attiecībā uz mākslīgā intelekta novērošanas pasākumiem apskatīta grāmatas sestajā nodaļā.

VDAR ir tieši piemērojama visās dalībvalstīs, un tā nav jāievieš nacionālajā regulējumā, tādējādi tiek izveidoti vienoti personas datu aizsardzības noteikumi, kas ir spēkā visā ES. Tajā pašā laikā VDAR ir paredzēti noteikumi, kurus var konkretizēt vai ierobežot ar dalībvalstu tiesību aktiem.[382] Tā satur vairāk nekā piecdesmit tā sauktās "atvērtās normas", kuras vai nu uzliek pienākumu dalībvalstīm pieņemt īpašus noteikumus[383], vai arī paredz dalībvalstīm rīcības brīvību un atļauj papildināt, konkretizēt vai paredzēt izņēmumus no VDAR[384]. Dalībvalstu tiesiskais regulējums nedrīkst traucēt VDAR noteikumu vienveidīgu piemērošanu visā ES.[385]

Latvija Fizisko personu datu apstrādes likumu (FPDAL) pieņēma 2018. gada 21. jūnijā.[386] FPDAL 8. nodaļā ir paredzēti specifiskie noteikumi un izņēmumi no datu subjektu tiesībām. Datu subjektam nav tiesību saņemt informāciju, ja to ir aizliegts izpaust saskaņā ar normatīvajiem aktiem, piemēram, nacionālās drošības, valsts aizsardzības, sabiedrības drošības un krimināltiesību jomā utt. (27. panta pirmā daļa). Ierobežots ir arī piekļuves tiesību īstenošanas termiņš – datu

382 VDAR 8. apsvērums.

383 Piemēram, noteikumi par rīcības kodeksiem – VDAR 40. pants, sertifikāciju – 42. pants, uzraudzības iestādes izveidi un pilnvarām – 54. pants un 58. panta 1. punkts.

384 Piemēram, normas, kas attiecas uz apstrādes tiesisko pamatu – VDAR 6. panta 2. un 3. punkts, bērna piekrišanu attiecībā uz informācijas sabiedrības pakalpojumiem – 8. panta 1. punkts, īpašo kategoriju personas datu apstrādi – 9. panta 2., 3., 4. punkts, personas datu par sodāmību un pārkāpumiem apstrāde – 10. pants, datu subjektu tiesību ierobežojumiem konkrētos gadījumos – 23. pants, apstrādi saistībā ar nodarbinātību – 88. pants.

385 VDAR 10. apsvērums. EST 1978. gada 31. janvāra spriedums lieta 94/77 *Fratelli Zerbone Snc pret Amministrazione delle finanze dello Stato*, ECLI:EU:C:1978:17, 25. punkts.

386 Fizisko personu datu apstrādes likums. Pieņemts 21.06.2018. *Latvijas Vēstnesis*, 04.07.2018., Nr. 132. Tas nosaka vispārīgos noteikumus (1. nodaļa), Datu valsts inspekcijas uzdevumus un statusu (2. nodaļa), inspekcijas darbības organizāciju (3. nodaļa), pārbaužu īstenošanas kārtību (4. nodaļa), noteikumus attiecībā uz datu aizsardzības speciālistiem (5. nodaļa), sertifikācijas un rīcības kodeksu pārraudzības institūcijas (6. nodaļa), lēmumu pieņemšanas, apstrīdēšanas un pārsūdzēšanas kārtību (7. nodaļa), datu apstrādi un datu subjekta tiesības (8. nodaļa).

subjekts var saņemt informāciju par tā datu saņēmējiem vai saņēmēju kategorijām, kam dati ir izpausti pēdējo divu gadu laikā (27. panta otrā daļa). FPDAL paredz speciālus noteikumus un datu subjektu tiesību ierobežojumus attiecībā uz īpašām apstrādes situācijām, piemēram, datu apstrādi saistībā ar vārda un informācijas brīvību (32. pants), kā arī datu apstrādi krimināltiesību jomā, nosakot, ka datu apstrāde sākotnēji neparedzētiem mērķiem krimināltiesību jomā ir pieļaujama, lai novērstu tūlītēju būtisku sabiedriskās drošības apdraudējumu, vai saskaņā ar speciālo regulējumu (34. pants). Speciālie noteikumi un izņēmumi var tikt paredzēti citos normatīvajos aktos, nodrošinot atbilstošas garantijas datu subjekta tiesībām un brīvībām un ievērojot VDAR noteiktās prasības.

4.2.4. Speciālais datu aizsardzības regulējums

Līdzās VDAR, kas paredz vispārīgo datu aizsardzības regulējumu, ES ir pieņēmusi vairākus speciālos tiesību aktus jeb *lex specialis*, kas konkretizē un papildina VDAR noteikumus.

Vienlaikus ar VDAR tika pieņemta Policijas direktīva, kuru dalībvalstīm ir pienākums ieviest nacionālajā regulējumā. Tā paredz speciālus noteikumus par personas datu apstrādi krimināllizmeklēšanas un tiesībaizsardzības nolūkos. Policijas direktīvas uzdevums ir stiprināt personu tiesību aizsardzību attiecībās ar tiesībaizsardzības iestādēm, kā arī efektīvāk apkarot noziedzību un terorismu visā ES, atvieglojot tiesībaizsardzības iestāžu pārrobežu sadarbību.

Lai pārņemtu Policijas direktīvas prasības, Latvija 2019. gada 8. jūlijā pieņēma likumu "Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā"[387]. Likuma mērķis ir aizsargāt fizisko personu pamattiesības un brīvības, it īpaši privātās dzīves neaizskaramību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus un administratīvos pārkāpumus, lai izpildītu krimināl sodus un administratīvos sodus, kā arī lai veiktu citas ar administratīvā pārkāpuma procesu un krimināl procesu saistītās darbības (2. pants). Likumu piemēro tikai attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes iepriekš minētajos nolūkos, savukārt, ja tiesību aizsardzības iestādes veic apstrādi citos nolūkos, uz to ir attiecināmas VDAR normas.

Speciālos datu aizsardzības noteikumus paredz arī Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi

387 Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā. LV likums. Pieņemts 08.07.2019. *Latvijas Vēstnesis*, 22.07.2019., Nr. 147.

un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (E-privātuma direktīva).[388]

E-privātuma direktīva aizsargā Hartas 7. pantā nostiprinātās tiesības uz privāto dzīvi, kuru būtiska sastāvdaļa ir elektronisko sakaru konfidencialitāte. Tās uzdevums ir garantēt elektronisko sakaru datu, aprīkojuma un pakalpojumu brīvu apriti ES. E-privātuma direktīva uzliek pienākumu publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem nodrošināt tīkla drošību, komunikāciju un informācijas par datu plūsmu konfidencialitāti. Tajā pašā laikā E-privātuma direktīva ir attiecināma tikai uz tradicionālajiem elektronisko sakaru pakalpojumiem, bet neattiecas uz jaunajiem elektronisko sakaru pakalpojumu sniedzējiem, piemēram, "WhatsApp", "Facebook Messenger", "Skype", "Gmail" u. c., kurus līdz ar tehnoloģiju progresu arvien vairāk izmanto kā patērētāji, tā uzņēmumi.

Speciālais datu aizsardzības regulējums attiecībā uz elektronisko sakaru konfidencialitātes aizsardzību, pārņemot E-privātuma direktīvas prasības, Latvijā tika ietverts Elektronisko sakaru likumā[389] un Informācijas sabiedrības pakalpojumu likumā[390]. Likums paredz elektronisko sakaru komersanta pienākumu nodrošināt saglabājamo datu glabāšanu 18 mēnešus un nodot tos tiesībaizsardzības iestādēm – pirmstiesas izmeklēšanas iestādēm, operatīvās darbības subjektiem, valsts drošības iestādēm, prokuratūrai un tiesai –, lai aizsargātu valsts un sabiedrisko drošību vai nodrošinātu noziedzīgu nodarījumu izmeklēšanu, kriminālvajāšanu un krimināllietu iztiesāšanu, kā arī Konkurences padomei, izmeklējot konkurences tiesību pārkāpumus, kas izpaužas kā aizliegtas vienošanās (19. panta pirmās daļas 11. punkts, 71.[1] pants).

Kā paredzēts 2015. gada Digitālajā vienotā tirgus stratēģijā Eiropai, 2016. gadā tika paziņots par E-privātuma direktīvas pārskatīšanu, lai nodrošinātu augsta līmeņa privātuma aizsardzību elektronisko sakaru pakalpojumu lietotājiem un vienlīdzīgus konkurences apstākļus visiem tirgus dalībniekiem, kā arī atbilstību VDAR.[391] 2017. gada 10. janvārī Eiropas Komisija pieņēma priekšlikumu Regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā, ar ko atceļ Direktīvu 2002/58/EK (E-privātuma regulas

388 Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektronisko komunikāciju). *OV L* 201, 31.07.2002.

389 Elektronisko sakaru likums. Pieņemts 28.10.2004. *Latvijas Vēstnesis*, 17.11.2004., Nr. 183.

390 Informācijas sabiedrības pakalpojumu likums. Pieņemts 04.11.2004. *Latvijas Vēstnesis*, 17.11.2004., Nr. 183.

391 Eiropas Komisija (2015), Komisijas paziņojums .. Digitālā vienotā tirgus stratēģija Eiropai.

priekšlikums).[392] E-privātuma regula konkretizēs un papildinās VDAR noteikumus attiecībā uz elektronisko sakaru datiem, kuri kvalificējami kā personas dati. Ar to paredzēts nodrošināt augstu aizsardzības līmeni gan saturam, gan metadatiem un paplašināt konfidencialitātes pienākumu, aptverot ne tikai tradicionālos sakaru pakalpojumus, bet arī citus esošos un nākotnes saziņas līdzekļus, tostarp piekļuvi internetam, tūlītējās ziņapmaiņas lietojumprogrammas, e-pastu, interneta tālruņa zvanus un personīgo ziņapmaiņu sociālajos medijos. Tā paredz regulēt sīkdatnes un piekrišanas noteikumus to izmantošanai. E-privātuma regulas pieņemšanas process ir ilgs, mēģinot panākt kompromisus un nodrošināt atbilstību VDAR. 2019. gadā EDRi kopā ar četrām citām pilsoniskās sabiedrības organizācijām uzsvēra steidzamu nepieciešamību pēc stingras E-privātuma regulas, lai risinātu problēmas, ko rada komerciālās novērošanas uzņēmējdarbības modeļi, un vērsa uzmanību, ka šie modeļi, kas balstīti uz cilvēku personīgās dzīves mirkļu izsekošanu, ir pārņēmuši internetu un radījuši stimulus, lai veicinātu dezinformāciju, manipulācijas un nelegālu saturu.[393] Gan Eiropas Datu aizsardzības uzraudzītājs, gan Eiropas Datu aizsardzības kolēģija atgādina, ka jaunajai regulai būtu jāsniedz vienāds vai augstāks aizsardzības līmenis nekā VDAR, nevis zemāks.[394]

Vēl ir arī daudzi citi speciālie tiesību akti, kas ietver datu aizsardzības noteikumus. 2018. gada oktobrī tika pieņemts jauns regulējums, kas ir piemērojams attiecībā uz personas datu apstrādi ES iestādēs un struktūrās – Regula Nr. 2018/1725[395]. Šādu apstrādi kontrolē Eiropas Datu aizsardzības uzraudzītājs. Datu aizsardzības noteikumus attiecībā uz konkrētām datu apstrādes darbībām tiesībaizsardzības jomā ietver arī Regula 2016/794 par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu), kas tiek uzskatīta par informācijas apmaiņas centru Eiropas

392 Eiropas Komisija. (2017). Priekšlikums. Eiropas Parlamenta un Padomes regula par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula). https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX:52017PC0010

393 Open letter to EU Member States. (11 October, 2019). *EDRi.* https://edri.org/files/eprivacy/ePrivacy_NGO_letter_20191011.pdf

394 Buttarelli, G. (19 October, 2018). The urgent case for a new ePrivacy law. *EDPS*. https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en; EDPB. (2019). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

395 Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK. *OV L* 295/39, 21.11.2018.

Savienībā.[396] Informācija, ko Eiropols vāc, glabā, apstrādā, analizē un ar ko tas apmainās, aptver kriminālizlūkošanu saistībā ar informāciju par noziegumiem vai noziedzīgām darbībām, kuru apkarošana ietilpst Eiropola mērķu darbības jomā, un informāciju, kura iegūta, lai noteiktu, vai ir izdarīti konkrēti noziedzīgi nodarījumi vai arī tie varētu tikt izdarīti nākotnē (12. apsvērums). Datu aizsardzības noteikumus ietver arī Padomes Regula (ES) 2017/1939, ar ko īsteno ciešāku sadarbību Eiropas Prokuratūras (EPPO) izveidei,[397] Regula (ES) 2018/1727 par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (Eurojust).[398]

Datu aizsardzības regulējumu ietekmē arī ES pieņemtais regulējums citās jomās, to skaitā kiberdrošībā. Drīz pēc VDAR pieņemšanas, 2016. gada jūlijā, tika pieņemta Direktīva 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (tā sauktā NIS direktīva)[399]. Lai pārņemtu minēto direktīvu, Latvija 2018. gadā veica būtiskus grozījumus 2010. gadā pieņemtajā Informācijas tehnoloģiju drošības likumā[400] un pieņēma 2015. gada Ministru kabineta noteikumus Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām".[401] 2019. gadā tika pieņemts Kiberdrošības akts, kas paredz ieviest ES mēroga kiberdrošības sertifikāciju, lai nodrošinātu, ka informāciju un komunikāciju tehnoloģiju produkti, pakalpojumi un procesi atbilst drošības standartiem, kā arī paredz stiprināt Eiropas Savienības Kiberdrošības aģentūras (ENISA) pilnvaras.[402]

396 Eiropas Parlamenta un Padomes Regula (ES) 2016/794 (2016. gada 11. maijs) par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu) un ar kuru aizstāj un atceļ Padomes Lēmumus 2009/371/TI, 2009/934/TI, 2009/935/TI, 2009/936/TI un 2009/968/TI. *OV L* 135, 24.05.2016.

397 Padomes Regula (ES) 2017/1939 (2017. gada 12. oktobris), ar ko īsteno ciešāku sadarbību Eiropas Prokuratūras (EPPO) izveidei. *OV L* 283, 31.10.2017.

398 Eiropas Parlamenta un Padomes Regula (ES) 2018/1727 (2018. gada 14. novembris) par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (Eurojust) un ar ko aizstāj un atceļ Padomes Lēmumu 2002/187/TI. *OV L* 295, 21.11.2018.

399 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā. *OJ L* 194, 19.07.2016.

400 Informācijas tehnoloģiju drošības likums. Pieņemts 28.10.2010. *Latvijas Vēstnesis*, 10.11.2010., Nr. 178.

401 MK noteikumi Nr. 442. Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām. Pieņemti 2015. gada 28. jūlijā. *Latvijas Vēstnesis*, 03.08.2015., Nr. 149.

402 Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (Dokuments attiecas uz EEZ). *OV L* 151, 07.06.2019.

Līdzās personas datu aizsardzības regulējumam Digitālā vienotā tirgus stratēģijas ietvaros ES ir pieņēmusi vairākus tiesību aktus, lai veicinātu uz datiem orientētas ekonomikas attīstību. 2018. gadā tika pieņemta Regula par nepersonalizētu datu brīvu apriti[403] un 2019. gadā – Direktīva par atvērtajiem datiem[404].

2020. gada februārī Eiropas Komisija pieņēma divus paziņojumus: Eiropas digitālās nākotnes veidošana[405], kā arī Eiropas datu stratēģiju[406], kas iepazīstina ar redzējumu par vienotu Eiropas datu telpu. Minētajos dokumentos tiek uzsvērts, ka tehnoloģiju, to skaitā mākslīgā intelekta, attīstībai, kā arī starptautiskajai sadarbībai šajā jomā ir jābalstās uz vērtībām un pamattiesībām, ieskaitot cilvēka cieņu, nediskrimināciju, privātās dzīves un datu aizsardzību.

2022. gada 30. maijā tika pieņemta Eiropas Parlamenta un Padomes Regula (ES) 2022/868 par Eiropas datu pārvaldību jeb Datu pārvaldības akts[407], kas paredz uzlabot nosacījumus datu kopīgošanai iekšējā tirgū, palielināt datu pieejamību un novērst tehniskos šķēršļus datu atkārtotai izmantošanai.

2022. gada februārī Eiropas Komisija publicēja Priekšlikumu Eiropas Parlamenta un Padomes regulai par saskaņotiem noteikumiem par taisnīgu piekļuvi datiem un to lietošanu (Datu aktu)[408], kura mērķis ir veicināt uzņēmumu un patērētāju labāku piekļuvi datiem un to izmantošanu, sniegt iespēju valsts iestādēm piekļūt privātā sektora datiem, ļaut klientiem pārslēgties starp dažādiem mākoņpakalpojumu sniedzējiem.

2020. gada 15. decembrī Eiropas Komisija nāca klajā ar Digitālo pakalpojumu akta pakotni, kas sastāvēja no divu regulu projektiem. Abas regulas tika

403 Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā. *OV L* 303/59, 28.11.2018. Regulas mērķis ir likvidēt šķēršļus brīvai datu pārrobežu plūsmai, jo īpaši dalībvalstu bieži piemērotos datu atrašanās vietas ierobežojumus. Tā kopā ar jau spēkā esošo personas datu aizsardzības regulējumu vairos juridisko noteiktību datu uzglabāšanas un citādas apstrādes pakalpojumu un darbību tirgū, ļaujot izmantot jauno tehnoloģiju radītās priekšrocības.

404 Eiropas Parlamenta un Padomes Direktīva (ES) 2019/1024 (2019. gada 20. jūnijs) par atvērtajiem datiem un publiskā sektora informācijas atkalizmantošanu. *OV L* 172, 26.06.2019.

405 Eiropas Komisija (2020). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Eiropas digitālās nākotnes veidošana. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52020DC0067

406 Eiropas Komisija (2020). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Eiropas Datu stratēģija. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52020DC0066

407 Eiropas Parlamenta un Padomes Regula (ES) 2022/868 (2022. gada 30. maijs) par Eiropas datu pārvaldību un ar ko groza Regulu (ES) 2018/1724 (Datu pārvaldības akts) (Dokuments attiecas uz EEZ). *OV L* 152, 03.06.2022.

408 Eiropas Komisija. (2020). Priekšlikums. Eiropas Parlamenta un Padomes regula par saskaņotiem noteikumiem par taisnīgu piekļuvi datiem un to lietošanu (Datu akts). https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52022PC0068

pieņemtas 2022. gada 5. jūlijā. Tās ir: Eiropas Parlamenta un Padomes Regula (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts)[409], ko piemēros no 2024. gada 17. februāra, un Eiropas Parlamenta un Padomes Regula (ES) 2022/1925 (2022. gada 14. septembris) par sāncensīgiem un godīgiem tirgiem digitālajā nozarē un ar ko groza Direktīvas (ES) 2019/1937 un (ES) 2020/1828 (Digitālo tirgu akts) [410], ko piemēro no 2023. gada 2. maija. Jaunais regulējums būs tieši piemērojams visās ES dalībvalstīs un radīs drošāku un atvērtāku digitālo vidi, kas balstās pamattiesībās. Tas ļaus cilvēkiem kontrolēt to, ko viņi redz internetā, lai tie nebūtu ierobežoti ar saturu, ko tiem izvēlas rādīt lielo tehnoloģiju platformu izstrādātie algoritmi.

Digitālo pakalpojumu akts nosaka skaidrus pienākumus digitālo pakalpojumu sniedzējiem, piemēram, sociālajiem medijiem un uzņēmumiem, kuri nodarbojas ar tiešsaistes tirdzniecību, lai novērstu nelikumīga, kaitīga un dezinformējoša satura izplatību. Jaunās prasības ir samērīgas ar platformu lielumu un riskiem, ko tās rada. Jaunā regula paredz pasākumus, lai cīnītos pret nelikumīgu saturu tiešsaistē, un uzliek platformām pienākumu ātri uz to reaģēt, vienlaikus ievērojot pamattiesības, tostarp vārda brīvību un datu aizsardzību. Tas paredz platformu pārredzamības un atbildības prasības, piemēram, pienākumu sniegt skaidru informāciju par satura moderēšanu un algoritmu izmantošanu satura ieteikšanai (tā sauktajām ieteikumu sistēmām). Digitālo pakalpojumu akts paredz nodrošināt lietotājiem efektīvus aizsardzības pasākumus, tostarp iespēju apstrīdēt platformu satura moderēšanas lēmumus, un nosaka obligāti sniedzamu informāciju lietotājiem, kad viņu saturs tiek izņemts vai ierobežots. Tas aizliedz maldinošu praksi, kuras mērķis ir manipulēt ar lietotāju izvēli, un noteikta veida mērķorientētas reklāmas, piemēram, izmantojot nepilngadīgo personu datus, kā arī sensitīvus datus. Ļoti lielām tiešsaistes platformām un meklētājprogrammām (ar 45 miljoniem vai vairāk ikmēneša lietotāju), būs jāievēro stingrāki pienākumi, ko uzraudzīs Eiropas Komisija, to skaitā jāanalizē un jānovērš sistēmiski riski (piemēram, nelikumīga satura izplatīšana; negatīva ietekme uz pamattiesībām; negatīva ietekme uz demokrātiskiem procesiem un sabiedrisko drošību; negatīva ietekme uz sabiedrības veselības aizsardzību un nepilngadīgajiem) un jāveic neatkarīga revīzija. Šīm lielajām platformām būs jāpiedāvā lietotājiem tāda satura ieteikšanas sistēma, kas nav balstīta uz viņu profilēšanu. Tām būs arī pienākums

409 Eiropas Parlamenta un Padomes Regula (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts) (Dokuments attiecas uz EEZ). *OV L* 227, 27.10.2022.

410 Eiropas Parlamenta un Padomes Regula (ES) 2022/1925 (2022. gada 14. septembris) par sāncensīgiem un godīgiem tirgiem digitālajā nozarē un ar ko groza Direktīvas (ES) 2019/1937 un (ES) 2020/1828 (Digitālo tirgu akts) (Dokuments attiecas uz EEZ). *OV L* 265, 12.10.2022.

atvieglot iestādēm un pētniekiem piekļuvi saviem datiem un algoritmiem, lai tos varētu pārbaudītu. Šis akts paredz būtiskus mehānismus, lai nodrošinātu platformu atbildību, tomēr ir daudzi izaicinājumi, kas saistīti ar tā ieviešanu un piemērošanu praksē.

Digitālo tirgu akts savukārt paredz noteikumus lielajām tiešsaistes platformām, kas darbojas kā vārtziņi jeb piekļuves kontrolieri (*gatekeepers* – angļu val.). Tā mērķis ir panākt, lai šīs platformas darbotos taisnīgi tiešsaistē, tādējādi nodrošinot taisnīgu komercvidi komerciālajiem lietotājiem, kuri ir atkarīgi no piekļuves kontrolieriem attiecībā uz savu pakalpojumu piedāvāšanu vienotajā tirgū, tehnoloģiju jaunuzņēmējiem, kā arī patērētājiem. Piemēram, šī regula aizliedz piekļuves kontrolieriem piemērot labvēlīgākus ierindošanas noteikumus pakalpojumiem un produktiem, kurus viņi piedāvā, salīdzinājumā ar citiem līdzīgiem pakalpojumiem un produktiem, ko piedāvā trešās personas viņu platformā. Šī regula arī papildina datu aizsardzības regulējumu, piemēram, attiecībā uz patērētāju profilēšanu, paredzot aizliegumu bez gala lietotāja iepriekšējas piekrišanas izsekot tos ārpus piekļuves kontrolieru pamatplatformas pakalpojuma, lai piedāvātu mērķorientētas reklāmas.

Lai gan ES datu aizsardzības reformas rezultātā ES ir pieņemti daudzi jauni tiesību akti, tajā pašā laikā tie neveido pilnīgi vienotu sistēmu. ES institūcijas, tāpat kā dalībvalstis, nav vēl pārskatījusi visus tiesību aktus, kas pieņemti pirms VDAR un Policijas direktīvas pieņemšanas un ietver speciālos datu aizsardzības noteikumus.[411] Turklāt datu aizsardzības regulējumu ietekmē jaunais regulējums, tai skaitā iepriekš aplūkotais Digitālo tirgu akts un Digitālo pakalpojumu akts. Datu aizsardzības regulējumu būtiski ietekmē arī mākslīgā intelekta regulējuma attīstība. ES uz pamattiesībām balstītā pieeja, kas ir pamatā datu aizsardzības regulējuma attīstībai, nosaka arī mākslīgā intelekta tehnoloģiju regulējuma turpmāko attīstību.

4.2.5. Mākslīgā intelekta regulējuma attīstība

Līdzīgi kā citas starptautiskās organizācijas, arī ES ir veikusi būtiskus soļus, lai izstrādātu mākslīgā intelekta ētisko un tiesisko regulējumu. 2018. gada aprīlī Eiropas Komisija publicēja paziņojumu "Mākslīgais intelekts Eiropai"[412] – pirmo ES mākslīgā intelekta stratēģiju, kas nosaka trīs galvenās prioritātes. Pirmkārt,

411 Sk. Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement; Drechsler, L. (2021). Wanted: LED adequacy decisions How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context, *International Data Privacy Law*, 11(2), pp. 182–195. https://doi.org/10.1093/idpl/ipaa019

412 Eiropas Komisija (2018), Komisijas paziņojums. Mākslīgais intelekts Eiropai.

veicināt ES tehnoloģisko attīstību un mākslīgā intelekta izmantošanu valsts un privātajā sektorā. Otrkārt, sagatavoties sociāli ekonomiskajām pārmaiņām, ko rada mākslīgais intelekts. Treškārt, izveidot atbilstošu ētisko un tiesisko regulējumu, pamatojoties uz ES vērtībām un saskaņā ar Hartu.

Mākslīgā intelekta kā ES līmeņa politikas prioritātes attīstība ir saistīta ar diskusiju, kā veicināt uzticēšanos mākslīgā intelekta sistēmām un kā nodrošināt, lai to izstrāde vai ieviešana neapdraud ES pamattiesības. Šie jautājumi patiesībā nav pilnīgi jauni, bet balstās iepriekšējās juridiskajās un politiskajās debatēs par pamattiesībām, un tie galvenokārt saistīti ar lielajiem datiem, kā arī vispārīgāk – ar datu apstrādes regulējumu.[413]

2018. gada 7. decembrī Eiropas Komisija pieņēma Mākslīgā intelekta koordinēto plānu[414], kas aicināja ES dalībvalstis sagatavot nacionālās stratēģijas mākslīgā intelekta jomā. Līdzīgi kā citas valstis, arī Latvija izstrādāja šādu stratēģiju. 2020. gada 4. decembrī Ministru kabinets apstiprināja Vides aizsardzības un reģionālās attīstības ministrijas sagatavoto informatīvo ziņojumu "Par mākslīgā intelekta risinājumu attīstību"[415].

ES uzsāka risināt mākslīgā intelekta ētiskos un juridiskos izaicinājumus, izveidojot divas darba grupas – AI HLEG un Atbildības un jauno tehnoloģiju ekspertu grupu. 2018. gada jūnijā tika izveidota AI HLEG, un 52 augsta līmeņa ekspertiem, kas tajā darbojās, tika uzticēts izstrādāt ieteikumus par mākslīgā intelekta politikas attīstību un ētiskiem, juridiskiem un sociāliem jautājumiem, kas nodrošinātu Eiropas mākslīgā intelekta stratēģijas un koordinētā plāna īstenošanu, pamatojoties uz cilvēku vērstu un ētisku pieeju mākslīgajam intelektam.

Pēc gada, 2019. gada aprīlī, AI HLEG pieņēma Ētikas vadlīnijas uzticamam mākslīgajam intelektam (MI ētikas vadlīnijas)[416]. Tajās ir uzsvērts – lai mākslīgā intelekta sistēmas varētu uzskatīt par uzticamām, tām ir jāatbilst trīs pazīmēm, proti, tām ir jābūt

1) likumīgām – jāievēro visi piemērojamie tiesību akti un pamattiesības;
2) ētiskām – jānodrošina ētikas principu un vērtību ievērošana;
3) noturīgām no tehniskā un sociālā viedokļa.

Lai mākslīgā intelekta sistēmas atbilstu ētiskuma pazīmei, tās ir jāizstrādā, jāievieš un jāizmanto, pamatojoties uz pamattiesībās balstītu pieeju un ievērojot

413 Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement.

414 Eiropas Komisija. (2018). Komisijas paziņojums Eiropas Parlamentam, Eiropadomei, Padomei, Eiropas Ekonomikas un Sociālajai komitejai un Reģionu komitejai. Koordinētais mākslīgā intelekta plāns. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52018DC0795&from=EN

415 VARAM (2020), Informatīvais ziņojums "Par mākslīgā intelekta risinājumu attīstību".

416 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

četrus ētikas principus: cilvēka patstāvība; kaitējuma novēršana; taisnīgums un izskaidrojamība.

MI ētikas vadlīnijas nosaka arī septiņas pamatprasības, kas ir jānodrošina, lai mākslīgā intelekta sistēmu izstrāde, ieviešana un izmantošana atbilstu uzticama mākslīgā intelekta prasībām:

1) cilvēka subjektība un virsvadība (cilvēka spēja pieņemt patstāvīgus lēmumus saistībā ar mākslīgo intelektu un šo sistēmu virsvadība);
2) tehniskā noturība un drošums;
3) privātums un datu pārvaldīšana;
4) pārredzamība;
5) daudzveidība, nediskriminēšana un taisnīgums;
6) vides un sabiedrības labklājība;
7) atbildīgums.

Pamatnostādnēs sniegts arī novērtēšanas saraksts, lai palīdzētu praktiski īstenot minētās prasības.

MI ētikas vadlīnijās kā viena no mākslīgā intelekta kritiskajām problēmjomām ir norādīta fizisku personu identificēšana un izsekošana, izmantojot mākslīgā intelekta sistēmas. Tās ļauj gan publiskām, gan privātām struktūrām arvien efektīvāk identificēt konkrētas personas. Vērā ņemami mākslīgā intelekta identifikācijas piemēri ir sejas atpazīšana un citas piespiedu identifikācijas metodes, kas izmanto biometriskos datus, piemēram, melu atpazīšana, personības vērtēšana ar mikroizpausmju palīdzību, automātiska balss atpazīšana. Dažkārt fizisku personu identificēšana ir vēlama un atbilst ētikas principiem, piemēram, ja to izmanto, lai atklātu krāpšanu, nelikumīgi iegūtu līdzekļu legalizāciju vai terorisma finansēšanu. Tomēr automātiska identificēšana raisa būtiskas juridiskas un ētiskas bažas, un tai var būt neparedzēta ietekme daudzos psiholoģiskos un sociālkulturālos līmeņos. Lai nosargātu Eiropas pilsoņu patstāvību, ir nepieciešams samērīgi izmantot mākslīgā intelekta kontroles paņēmienus. Uzticama mākslīgā intelekta sasniegšanai būs ļoti svarīgi skaidri definēt, vai, kad un kā mākslīgo intelektu var izmantot, lai automātiski identificētu cilvēkus, un nošķirt personas identificēšanu no tās izsekošanas, kā arī mērķtiecīgu novērošanu no masveida novērošanas. Šādu tehnoloģiju izmantošana ir skaidri jāpamato saskaņā ar spēkā esošajiem tiesību aktiem.

MI ētikas vadlīnijās kā vēl viena problēmjoma tiek norādīta mākslīgā intelekta atbalstīta iedzīvotāju vērtēšana, kas pārkāpj pamattiesības. Jebkāda iedzīvotāju vērtēšana var novest pie patstāvības zaudējuma un apdraudēt nediskriminēšanas principu. Vērtēšana būtu jāizmanto tikai tad, ja tā ir pamatota un ja pasākumi ir samērīgi un taisnīgi. Valsts iestāžu vai privātā sektora veikta iedzīvotāju vērtēšana (vispārējs "morālās personības" vai "ētiskās godprātības" vērtējums) visos aspektos un plašā mērogā apdraud šīs vērtības, jo īpaši, ja to neizmanto saskaņā

ar pamattiesībām vai ja to izmanto nesamērīgi, bez skaidri noteikta un paziņota leģitīmā mērķa.

2019. gada aprīlī kopā ar MI ētikas vadlīniju pārskatīto versiju tika publicēts Eiropas Komisijas paziņojums "Uzticības veidošana uz cilvēku vērstam mākslīgajam intelektam"[417], kas uzsāka visaptverošu izmēģināšanas procesu, iesaistot plašu ieinteresēto personu loku, lai pārbaudītu MI vadlīniju praktisku īstenošanu mākslīgā intelekta sistēmu izstrādē un izmantošanā.

2019. gada jūnijā AI HLEG publicēja otru dokumentu – "Politikas un ieguldījumu ieteikumi uzticamam mākslīgajam intelektam"[418], kas sniedz ieteikumus ES iestādēm un dalībvalstīm, kā attīstīt, ieviest un veicināt mākslīgā intelekta izmantošanu un konkurētspēju Eiropā.

2020. gada 17. jūlijā AI HLEG pēc plašas sabiedriskās apspriešanas, diskusijām Eiropas Mākslīgā intelekta aliansē, kā arī izmēģināšanas procesa, kurā piedalījās vairāk nekā 350 organizācijas, publicēja Uzticama mākslīgā intelekta novērtēšanas saraksta gala versiju – praktisku rīku, lai palīdzētu uzņēmumiem un organizācijām pašām novērtēt to izstrādāto mākslīgā intelekta sistēmu atbilstību MI ētikas vadlīnijās noteiktajām septiņām uzticama mākslīgā intelekta prasībām.[419] Tas ir izstrādāts, stingri balstoties uz cilvēku pamattiesību aizsardzību. Dokumentā ir uzsvērts, ka ir jānovērtē mākslīgā intelekta sistēmu ietekme uz tādām pamattiesībām kā cilvēka cieņa, diskriminācijas aizliegums, tiesības uz privātumu un datu aizsardzību. Datu pārvaldības prasība paredz novērtēt datu aizsardzības noteikumu, kas izriet no VDAR, ievērošanu, piemēram, vai ir veikts novērtējuma par ietekmi uz datu aizsardzību, vai ir iecelts datu aizsardzības speciālists, vai pastāv uzraudzības mehānisms pār datu apstrādi, vai ir īstenoti pasākumi, lai nodrošinātu privātumu pēc noklusējuma un integrētu datu aizsardzību, minimizēšanas principa ievērošanu, vai, izstrādājot mākslīgā intelekta sistēmas, ir izmantotas tiesības atsaukt piekrišanu, tiesības iebilst un tiesības tikt aizmirstam.

Lai gan daudzas MI ētikas vadlīnijās ietvertās prasības izriet no spēkā esošām pamattiesībām, kā arī citiem tiesību aktiem, tajā pašā laikā tās nav juridiski saistošas. Turklāt tajās ir ietverta tikai daļa no VDAR izrietošajām prasībām.

417 European Commission. (2019). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Building Trust in Human Centric Artificial Intelligence. https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence

418 AI HLEG. (2019). Policy and investment recommendations for trustworthy Artificial Intelligence. https://www.europarl.europa.eu/italy/resource/static/files/import/intelligenza_artificiale_30_aprile/ai-hleg_policy-and-investment-recommendations.pdf

419 AI HLEG. (2020). Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment. https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

Eiropas Komisija 2020. gada 19. februārī publicēja Balto grāmatu par mākslīgo intelektu[420], kurā izklāstīti iespējamie mākslīgā intelekta tiesiskā regulējuma attīstības virzieni. Tā iepazīstina ar mākslīgā intelekta attīstības redzējumu, kas balstās uz izcilību un uzticēšanos. Tā apstiprina, ka ir jāīsteno un sinerģiski jāintegrē divi paralēli mākslīgā intelekta politikas mērķi. No vienas puses, jāveicina mākslīgā intelekta izpēte un ieviešana, lai ES būtu konkurētspējīga ar ASV un Ķīnu. Jācenšas mobilizēt resursus, lai panāktu "izcilības ekosistēmu", kas radītu pareizos stimulus, lai paātrinātu ekonomisko attīstību un lai Eiropa būtu piemērota digitālajam laikmetam un pozicionētos kā pasaules līdere ilgtspējīgu tehnoloģisko inovāciju jomā. No otras puses, mākslīgā intelekta tehnoloģiju ieviešanai būtu jāatbilst ES pamattiesībām un sociālajām vērtībām, radot uzticību. Kā norāda politoloģijas profesors Džovanni Sartors (*Giovanni Sartor*), ir svarīgi uzsvērt, ka abi mērķi ir savienojami, bet atšķirīgi. No vienas puses, visprogresīvākās mākslīgā intelekta lietojumprogrammas varētu izmantot, kaitējot pilsoņu tiesībām un sociālajām vērtībām. No otras puses, efektīva pilsoņu aizsardzība pret riskiem, ko rada mākslīgā intelekta ļaunprātīga izmantošana, pati par sevi nenodrošina stimulus, kas vajadzīgi, lai veicinātu pētniecību un inovāciju un lietderīgu mākslīgā intelekta izmantošanu.[421]

Lai radītu uzticēšanos mākslīgajam intelektam, ir jānodrošina tā atbilstība ES tiesiskajam regulējumam, ieskaitot pamattiesību un patērētāju tiesību regulējumu, it sevišķi attiecībā uz mākslīgā intelekta sistēmām, kas darbojas ES un rada augstu risku jeb bīstamību. Mākslīgā intelekta sistēmu izmantošana būtiskākos riskus rada tādu noteikumu piemērošanai, kuru mērķis ir aizsargāt pamattiesības, ieskaitot personas datu un privātuma aizsardzību, diskriminācijas aizlieguma principu, tiesības uz efektīvu tiesisko aizsardzību, kā arī patērētāju aizsardzību.

Baltā grāmata mudina izstrādāt jaunu mākslīgā intelekta tiesisko regulējumu un pieņemt juridiski saistošas prasības gadījumos, kad mākslīgā intelekta izmantošana rada augstu risku. Šis risks ir izsverams, izvērtējot, vai nozare un paredzētais izmantošanas veids nes līdzi būtisku apdraudējumu, sevišķi drošības, patērētāja tiesību un pamattiesību aizsardzības aspektā. Turklāt atsevišķos izņēmuma gadījumos mākslīgā intelekta izmantošana konkrētiem mērķiem pati par sevi ir uzskatāma par stipri bīstamu neatkarīgi no nozares. Viens no šādiem gadījumiem, kad mākslīgā intelekta izmantošana rada augstu risku, ir "biometriska attālināta identifikācija un citas uzbāzīgas novērošanas tehnoloģijas". Baltajā grāmatā ir norādīts, ka attiecībā uz mākslīgā intelekta izmantošanu, kas rada augstu risku, tiesiskajā regulējumā nosakāmās prasības varētu attiekties uz apmācību

420 Eiropas Komisija (2020), Baltā grāmata par mākslīgo intelektu.

421 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

datiem, datu un uzskaites glabāšanu, sniedzamo informāciju, noturību un precizitāti, cilvēka virsvadību, kā arī varētu tikt paredzētas īpašas prasības dažiem mākslīgā intelekta izmantošanas veidiem, piemēram, biometriskajai attālinātajai identifikācijai.

Līdzās pamattiesībām mākslīgais intelekts rada arī jautājumus, kā garantēt tā drošumu un tiesisko atbildību. Baltajai grāmatai par mākslīgo intelektu ir pievienots Ziņojums par mākslīgo intelektu, lietu internetu un robotiku drošuma un atbildības aspektā[422], kurā tiek analizēts spēkā esošais tiesiskais regulējums, lai novērtētu, vai un cik daudz pašreizējais regulējums par drošību un atbildību joprojām ir piemērots lietotāju aizsardzībai. Tas ir izstrādāts, balstoties uz Ekspertu grupas atbildības un jauno tehnoloģiju jomā 2019. gada novembrī publicēto Ziņojumu par mākslīgā intelekta un citu jauno tehnoloģiju atbildību, un sniedz ieteikumus par to, kā būtu jāizstrādā vai jāatjaunina atbildības režīmi ES, lai risinātu problēmas, kas izriet no straujajām tehnoloģiju izmaiņām.[423]

2020. gada 23. jūlijā Eiropas Komisija publicēja Sākotnējo ietekmes novērtējumu Priekšlikumam Eiropas Parlamenta un Padomes tiesību aktam, ar ko nosaka prasības mākslīgajam intelektam.[424] Tas papildina Balto grāmatu par mākslīgo intelektu, turpinot izvērtēt attiecīgās politikas iespējas un politikas instrumentus.

2020. gada 20. oktobrī Eiropas Parlaments pieņēma priekšlikumus par ES mākslīgā intelekta regulējuma izveidi attiecībā uz mākslīgā intelekta ētiku, atbildību par mākslīgā intelekta radīto kaitējumu un intelektuālā īpašuma tiesībām. Eiropas Parlaments rezolūcijā ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru mudina Eiropas Komisiju iesniegt jaunu tiesisko regulējumu un piedāvā priekšlikuma tekstu Regulai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrādes, ieviešanas un izmantošanas ētikas principiem.[425]

Eiropas Parlamenta piedāvātajā mākslīgā intelekta regulas priekšlikumā kā mērķis tika noteikts izveidot visaptverošu un nākotnes prasībām atbilstošu ES ētikas principu un juridisko pienākumu tiesisko regulējumu, saskaņā ar kuru ES

422 Eiropas Komisija. (2020). Komisijas ziņojums Parlamentam, Padomei un Eiropas Ekonomikas un sociālo lietu komitejai. Ziņojums par mākslīgo intelektu, lietu internetu un robotiku drošuma un atbildības aspektā. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020DC0064&from=en

423 European Commission. Expert Group on Liability and New Technologies – New Technologies Formation. (2019). Liability for Artificial Intelligence and Other Emerging Digital Technologies. https://op.europa.eu/publication/manifestation_identifier/PUB_DS0319853ENN

424 European Commission. (2020). Inception Impact Assessment. Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Requirements-for-Artificial-Intelligence

425 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

tiktu īstenota mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrāde, ieviešana un izmantošana (1. pants). Tajā tika noteikti vairāki būtiski principi, tostarp:

- uz cilvēku orientēts, cilvēku radīts un cilvēku kontrolēts mākslīgais intelekts, robotika un saistītās tehnoloģijas;
- obligāta augsta riska mākslīgā intelekta, robotikas un saistīto tehnoloģiju atbilstības novērtēšana;
- drošība, pārredzamība un pārskatatbildība;
- aizspriedumu un diskriminācijas nepieļaušana;
- tiesības uz tiesisko aizsardzību;
- sociālā atbildība un dzimumu vienlīdzība;
- vides ilgtspēja, privātās dzīves neaizskaramība un personas datu aizsardzība;
- biometriskās atpazīšanas izmantošanas ierobežojumi, laba pārvaldība.

Pirmajā nodaļā tika iekļauti vispārīgie noteikumi, kas paredz regulas pieņemšanas nolūku (1. pants), piemērošanas jomu (2., 3. pants), definīcijas (4. pants), kā arī vispārīgus noteikumus par ētikas principiem (5. pants). Otrajā nodaļā tika noteikti pienākumi attiecībā uz augsta riska tehnoloģijām, nosakot iepriekš minētos ētikas principus, pienākumu veikt riska novērtējumu (14. pants), atbilstības novērtēšanu (15. pants), kā arī paredzēti noteikumi attiecībā uz Eiropas ētiskās atbildības sertifikātu (16. pants). Tas paredzēja it īpaši regulēt augsta riska tehnoloģijas. Priekšlikuma pielikumā tika ietverts izsmeļošs un kumulatīvs augsta riska nozaru un augsta riska izmantošanas veidu un mērķu saraksts. Trešā nodaļa ietvēra institucionālās pārraudzības noteikumus, cita starpā nosakot pienākumu nodrošināt mākslīgā intelekta atbilstību pārvaldības standartiem, to skaitā attiecībā uz datiem, piemēram, veicot ārējo datu kvalitātes pārbaudes (17. pants), neatkarīgas uzraudzības iestādes izveidi katrā dalībvalstī (18. pants), kā arī ziņošanu par pārkāpumiem un ziņojošo personu aizsardzību (19. pants).

Eiropas Parlamenta piedāvātajā regulas priekšlikumā tika ietverti vispārīgi noteikumi par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētikas principiem, uzsverot vispārīgo pienākumu ikvienā gadījumā ievērot ES tiesību aktus un Hartā noteiktās pamattiesības (5. pants). Pirmkārt, tajā tika uzsvērts, ka jebkurš mākslīgais intelekts, robotika un saistītās tehnoloģijas, tostarp programmatūras, algoritmi un šādu tehnoloģiju izmantotie vai ģenerētie dati, ES ir jāizstrādā, jāievieš un jāizmanto saskaņā ar ES tiesību aktiem un pilnībā ievērojot cilvēka cieņu, autonomiju un drošību un citas Hartā noteiktas pamattiesības (5. panta 1. punkts). Otrkārt, tika akcentēts, ka tādu personas datu apstrādi, kas ir iegūti, izstrādājot, ieviešot un izmantojot mākslīgo intelektu, robotiku un saistītās tehnoloģijas, tostarp tādu personas datu apstrādi, kuru avots ir nepersonas dati un biometriskie dati, veic saskaņā ar VDAR un E-privātuma direktīvu. ES izstrādātam, ieviestam un izmantotam mākslīgajam intelektam, robotikai un saistītajām tehnoloģijām, tostarp programmatūrai, algoritmiem un šādu tehnoloģiju

izmantotiem vai ģenerētiem datiem, ir jābūt pilnīgā saskaņā ar ES pilsoņu tiesībām uz privātumu un personas datu aizsardzību (preambulas 35. punkts).

Priekšlikumā tika paredzētas prasības attiecībā uz biometriskās attālinātās atpazīšanas izmantošanu. Tajā tika noteikts privātās dzīves neaizskaramības un personas datu aizsardzības princips, kas paredz, ka biometrisko datu izmantošana un vākšana attālinātās identifikācijas nolūkos publiskās vietās, izmantojot biometrisko vai sejas atpazīšanu, īpaši apdraud pamattiesības, un to ievieš vai izmanto tikai dalībvalstu publiskās iestādes, aizstāvot būtiskas sabiedrības intereses. Minētās iestādes nodrošina, ka šādu pasākumu ieviešana vai izmantošana tiek darīta zināma sabiedrībai, ir samērīga, mērķtiecīga un aprobežojas ar konkrētiem mērķiem un atrašanās vietu un ir ierobežota laikā saskaņā ar ES un valstu tiesību aktiem, jo īpaši VDAR un E-privātuma direktīvu, un šajā ieviešanā un izmantošanā pienācīgi ņem vērā cilvēka cieņu un autonomiju, kā arī Hartā noteiktās pamattiesības, proti, tiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību (12. pants).

Tajā pašā laikā Eiropas Parlamenta regulas priekšlikums neparedzēja aizliegumus jeb sarkanās līnijas mākslīgā intelekta sejas atpazīšanas vai citu biometriskās attālinātās atpazīšanas sistēmu izmantošanai, kā arī cita veida mākslīgā intelekta novērošanas sistēmu izmantošanai. Tas neaizliedza tiesībaizsardzības iestādēm tās izmantot, atsaucoties uz sabiedrības vai valsts drošības interesēm, bet izvirzīja noteiktas prasības, atstājot tām rīcības brīvību izvērtēt atbilstību.

2021. gada 21. aprīlī Eiropas Komisija nāca klajā ar jaunu MI akta priekšlikumu[426], kas ir uzskatāms par ļoti nozīmīgu soli, jo tas ir pirmais priekšlikums pasaulē, kas paredz mākslīgā intelekta jomas tiesisko regulējumu. MI akta priekšlikums nosaka saskaņotus noteikumus mākslīgā intelekta sistēmu izmantošanai ES. Tas aizliedz noteiktus mākslīgā intelekta izmantošanas veidus, nosaka īpašas prasības augsta riska mākslīgā intelekta sistēmām, pārredzamības noteikumus mākslīgā intelekta sistēmām, kas paredzētas mijiedarbībai ar fiziskām personām, kā arī tirgus uzraudzības un mākslīgā intelekta sistēmu atbilstības uzraudzības noteikumus (1. pants).

Mākslīgā intelekta sistēmas ir paredzēts regulēt atkarībā no riska, ko tās rada, iedalot tās četrās dažādās riska kategorijas: mākslīgā intelekta sistēmas, kas rada minimālu risku, ierobežotu risku, augstu risku vai nepieņemamu risku.

MI akta priekšlikums paredz vairākus aizliegumus izmantot mākslīgā intelekta sistēmas, kuras uzskatāmas par nepieņemamām, jo ir pretrunā ar pamattiesībām un Eiropas vērtībām (5. pants). Pirmkārt, tas aizliedz praksi, kurai var būt ievērojams potenciāls manipulēt ar personām. Proti, ir aizliegta tādas mākslīgā intelekta sistēmas laišana tirgū, nodošana ekspluatācijā vai lietošana, kura

426 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

izmanto subliminālus paņēmienus, lai, personām to neapzinoties, būtiski iespaidotu personas uzvedību tādā veidā, kas šai vai citai personai rada vai var radīt fizisku vai psiholoģisku kaitējumu (5. panta 1. punkta a) apakšpunkts). Tāpat ir aizliegts izmantot noteiktu neaizsargātu grupu, piemēram, bērnu vai personu ar invaliditāti, neaizsargātības iezīmes, lai būtiski ietekmētu šai grupai piederīgas personas uzvedību tā, ka šai vai citai personai tiek vai var tikt radīts fizisks vai psiholoģisks kaitējums, piemēram, rotaļlietas-virtuālos palīgus, kas mudina bērnus uz bīstamu rīcību (5. panta 1. punkta b) apakšpunkts).

MI akta priekšlikums aizliedz sistēmas, kas ļauj valsts iestādēm veikt "sociālo novērtēšanu" vispārējiem mērķiem. Proti, ir aizliegta tādu mākslīgā intelekta sistēmu laišana tirgū, nodošana ekspluatācijā vai lietošana, ko veic publiskā sektora iestādes vai to vārdā fiziskas personas, lai izvērtētu vai klasificētu fizisku personu uzticamību noteiktā laikposmā, pamatojoties uz viņu sociālo uzvedību vai zināmām vai prognozētām personas vai personības īpašībām, ja sociālais novērtējums ved pie viena vai abiem šādiem iznākumiem (5. panta 1. punkta c) apakšpunkts). Šāda sociālā novērtēšanas sistēma pastāv Ķīnā, kur valsts vara ir ieviesusi plašu mākslīgā intelekta novērošanas sistēmu, kopā ar tā saukto sociālo kredīta sistēmu, lai kontrolētu iedzīvotājus, kas darbojas pretrunā ar demokrātiskām vērtībām.

Priekšlikums paredz aizliegt izmantot tiesībaizsardzības nolūkos reāllaika biometriskās attālinātās identifikācijas sistēmas sabiedriskās vietās (5. panta 1. punkta d) apakšpunkts). Tajā pašā laikā ir paredzēti arī vairāki izņēmuma gadījumi, kad šāda izmantošana ir atļauta, piemēram, ja tas ir nepieciešams smagu noziedzīgu nodarījumu atklāšanai. Visas pārējās fizisko personu attālinātās biometriskās identifikācijas sistēmas, ko izmanto valsts iestādes citos nolūkos vai privātie uzņēmumi, ir uzskatāmas par augsta riska sistēmām.

Cilvēktiesību aizstāvības organizācijas šiem noteikumiem ir veltījušas plašu kritiku.[427] Eiropas Datu aizsardzības uzraudzītājs vērš uzmanību, ka sarkanās līnijas būtu jānosaka stingrāk un jāaizliedz arī citas augsta riska biometriskās atpazīšanas sistēmas, piemēram, emociju uztveršanas sistēmas.[428]

MI akta priekšlikums paredz īpašus noteikumus mākslīgā intelekta sistēmām, kas rada augstu risku saskaņā ar 6. pantu, kā arī III pielikumu, kurā ir uzskaitītas daudzas jomas, kurās mākslīgā intelekta sistēmas uzskatāmas par augsta riska sistēmām. Šajā kategorijā cita starpā ietilpst fizisku personu biometriskā

427 EDRi. EU's AI law needs major changes to prevent discrimination and mass surveillance. https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/

428 EDPS. (23 April, 2021). Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary. https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en

identifikācija un kategorizācija, t. i. mākslīgā intelekta sistēmas, ko paredzēts izmantot fizisku personu attālinātai identifikācijai reāllaikā un vēlāklaikā. Augstu risku rada arī mākslīgā intelekta sistēmas, ko paredzēts izmantot tiesībaizsardzības iestādēs:

- sistēmas, kas paredzētas, lai veiktu individuālus riska novērtējumus, kuros vērtē risku, ka fiziska persona izdarīs pārkāpumu vai atkārtotu pārkāpumu, vai risku, kam pakļauti iespējamie noziedzīgos nodarījumos cietušie;
- sistēmas, ko paredzēts izmantot kā melu detektorus vai līdzīgus rīkus vai nolūkā noteikt fiziskas personas emocionālo stāvokli;
- mākslīgā intelekta sistēmas, ko paredzēts izmantot faktiska vai potenciāla noziedzīga nodarījuma izdarīšanas vai atkārtošanas prognozēšanai, pamatojoties uz fizisku personu profilēšanu vai fizisku personu vai grupu personības un rakstura īpašību vai agrākas noziedzīgas rīcības novērtēšanu;
- mākslīgā intelekta sistēmas, ko paredzēts izmantot fizisku personu profilēšanai noziedzīgu nodarījumu atklāšanas, izmeklēšanas vai kriminālvajāšanas gaitā;
- sistēmas, ko paredzēts izmantot noziegumu analīzei attiecībā uz fiziskām personām un kas ļauj tiesībaizsardzības iestādēm veikt meklēšanu lielās, kompleksās saistītu un nesaistītu datu kopās, kuras pieejamas dažādos datu avotos vai dažādos datu formātos, lai datos atklātu nezināmus modeļus vai slēptas sakarības.

Augstu risku rada arī mākslīgā intelekta izmantošana daudzās citās jomās, piemēram, migrācijas, patvēruma un robežkontroles pārvaldības jomā.

Augsta riska mākslīgā intelekta sistēmām ir piemērojamas stingras prasības. MI akta priekšlikums paredz pienākumu ieviest riska novērtēšanas sistēmu, lai noteiktu zināmus un paredzamus mākslīgā intelekta riskus, kā arī to samazināšanas un uzraudzības pasākumus. Attiecībā uz augsta riska mākslīgā intelekta sistēmām ir noteiktas prasības, kas attiecas uz izmantoto datu kopu kvalitāti, tehnisko dokumentāciju un uzskaiti, pārredzamību un informācijas sniegšanu lietotājiem, cilvēka virsvadību un noturību, precizitāti un kiberdrošību.

Regulas priekšlikums paredz arī detalizētus noteikumus par to, kā tiks uzraudzīta MI sistēmu atbilstība gan ES, gan valsts līmenī. Ir paredzēts izveidot Eiropas Mākslīgā intelekta padomi, un arī Latvijā būs jānozīmē atbildīgā uzraudzības institūcija. Eiropas līmenī tiks izveidota augsta riska mākslīgā intelekta sistēmu datubāze.

Mēs šobrīd nedzīvojam "tiesiskā vakuumā". Jaunais mākslīgā intelekta regulējums mēģina novērst trūkumus esošajā regulējumā. Jau šobrīd mākslīgā intelekta sistēmas regulē daudzi spēkā esošie tiesību akti, īpaši cilvēktiesību regulējums un datu aizsardzības noteikumi. Regulas horizontālā pieeja prasa nodrošināt tās

pilnīgu atbilstību spēkā esošajam ES tiesiskajam regulējumam attiecībā uz sektoriem, kuros tiek izmantotas augsta riska mākslīgā intelekta sistēmas.

Līdz šim diskusijas par mākslīgā intelekta regulējumu dziļi balstījās ES digitālā vienotā tirgus programmā, un, kaut arī tās var atsaukties uz nepieciešamību ņemt vērā tiesībaizsardzības un krimināltiesiskās īpatnības, šādas politikas diskusijas visbiežāk nav balstītas uz detalizētu šo jomu pārskatu un neņem vērā konkrētus piemērojamos noteikumus, it īpaši ierobežojumus un atkāpes.[429]

Tajā pašā laikā gan starptautiskā, gan ES līmenī arvien skaidrāk tiek pieprasīts skaidrs tiesiskais regulējums, kas noteiktu ierobežojumus, aizsardzības garantijas un prasības, to skaitā arī sarkanās līnijas attiecībā uz mākslīgā intelekta novērošanas tehnoloģiju izmantošanu.

Kā tika atklāts iepriekš, starptautiskās organizācijas – Eiropas Padome un ANO – jau ilgstoši ir mudinājušas pārskatīt starptautisko, kā arī nacionālo regulējumu, stiprināt datu aizsardzības standartus un nodrošināt efektīvas aizsardzības garantijas attiecībā uz masveida digitālās novērošanas pasākumiem. Sniegtie ieteikumi ir lielā mērā piemērojami arī attiecībā uz mākslīgā intelekta novērošanas tehnoloģijām. Daudzi no priekšlikumiem, kas sniegti iepriekš attiecībā uz digitālās novērošanas pasākumu regulējumu, šobrīd ir atrodami mākslīgā intelekta vadlīnijās, piemēram, nepieciešamība ievērot samērīguma principu, nodrošināt pārredzamību un atbildību. ES līmenī vislielākie nopelni masveida novērošanas ierobežošanā ir EST, kuras lēmumi ir vairākkārt likuši pārskatīt spēkā esošo regulējumu. Nākamajā nodaļā detalizētāk atklāts, kādas prasības cilvēktiesību ierobežošanai, piemērojot masveida novērošanas pasākumus, paredz starptautiskais cilvēktiesību regulējums un pārnacionālo tiesu – EST un ECT – izveidotā prakse. Atklāts, ka abas tiesas ir izstrādājušas būtiskas prasības, kas piemērojamas attiecībā arī uz mākslīgā intelekta tehnoloģijām un var palīdzēt nodrošināt to ētisku un atbildīgu izmantošanu, izvērtēt to samērīgumu un nepieciešamību, kā arī noteikt novērošanas tehnoloģiju izmantošanas robežas.

429 Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights.

5. DAĻA

Tiesību uz privātumu un datu aizsardzību ierobežošana: Eiropas tiesu prakse masveida novērošanas lietās

Izmantojot mākslīgā intelekta sistēmas, ir jāievēro cilvēktiesības, īpaši tiesības uz privātumu un datu aizsardzību. Mākslīgā intelekta, kā arī citi masveida novērošanas pasākumi būtiski apdraud cilvēktiesības. Tāpēc jautājums ir, kā noteikt robežas, cik tālu valsts var īstenot šādus pasākums, un kādi nosacījumi un garantijas ir jāievēro, lai cilvēktiesību ierobežojumi būtu samērīgi un likumīgi. Uz šo jautājumu ilgstoši ir centušās atbildēt divas Eiropas pārnacionālās tiesas – EST un ECT, izveidojot plašu tiesu praksi masveida novērošanas lietās. Šo tiesu nolēmumi, kuros ir analizēti cilvēktiesību ierobežošanas nosacījumi un nepieciešamās aizsardzības garantijas, kas ir jāpiemēro masveida novērošanas pasākumiem, ir svarīgs avots, lai varētu izvērtēt, vai valstu prakse nepārkāpj cilvēktiesības, arī gadījumos, kad tiek ieviesti un īstenoti mākslīgā intelekta novērošanas pasākumi.

Grāmatas turpinājumā vispirms sniegts ieskats, kādi ir cilvēktiesību dokumentos noteiktie tiesību uz privātumu un datu aizsardzību ierobežošanas nosacījumi. Pēc tam nodaļā aplūkots, kā šos nosacījumus ir piemērojusi ECT un EST masveida novērošanas lietās – kādas prasības un aizsardzības garantijas tās ir atzinušas par būtiskām, un kā tās būtu piemērojamas mākslīgā intelekta novērošanas tehnoloģijām, lai to ieviešana un izmantošana nepārkāptu tiesības uz privātumu un datu aizsardzību.[430]

5.1. Tiesību uz privātumu un datu aizsardzību ierobežošanas nosacījumi

Pastāv absolūtas cilvēktiesības, kuras nekādā gadījumā nevar ierobežot, piemēram, tiesības uz dzīvību. Tomēr lielāko daļu cilvēktiesību, tostarp tiesības uz privātumu un tiesības uz datu aizsardzību, var ierobežot. Tomēr šāda ierobežošana ir pieļaujama, tikai ievērojot konkrētus nosacījumus jeb ierobežošanas kritērijus.

Cilvēktiesību ierobežojumu kritēriji ir noteikti cilvēktiesību dokumentos. Gadījumi, kādos valsts var ierobežot tiesības uz privāto dzīvi, ir noteikti ECTK 8. panta 2. punktā: "Publiskās institūcijas nedrīkst traucēt nevienam baudīt šīs tiesības, izņemot gadījumus, kas ir paredzēti likumā un ir nepieciešami demokrātiskā sabiedrībā, lai aizsargātu valsts vai sabiedrisko drošību vai valsts

430 Grāmatā aplūkoti spriedumi, kurus EST un ECT ir pieņēmusi līdz 2021. gada aprīlim.

ekonomiskās labklājības intereses, lai nepieļautu nekārtības vai noziegumus, lai aizsargātu veselību vai tikumību, vai lai aizstāvētu citu tiesības un brīvības."

Saskaņā ar minēto normu tādas intereses kā valsts un sabiedriskā drošība, kā arī veselības aizsardzība ir pamats, lai varētu ierobežot cilvēktiesības. Tomēr šādi ierobežojumi ir pieļaujami tikai tad, ja tie ir "paredzēti likumā" un ir "nepieciešami demokrātiskā sabiedrībā", lai aizsargātu kādu no leģitīmajiem mērķiem. Pēdējais nosacījums arī paredz, ka iejaukšanās tiesībās ir jābūt proporcionālai izvirzītajam mērķim un ka šī mērķa sasniegšanai jāizraugās vismazāk ierobežojošais līdzeklis.[431]

Minētie cilvēktiesību ierobežošanas nosacījumi ir atrodami arī citos cilvēktiesību dokumentos. Hartas 7. un 8. pantā noteiktās tiesības uz privātumu un datu aizsardzību var ierobežot, ievērojot tiesību un brīvību ierobežošanas kritērijus. Šie kritēriji ir paredzēti Hartas 52. panta 1. punktā, kas nosaka: "Visiem šajā Hartā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jābūt noteiktiem tiesību aktos, un tajos jārespektē šo tiesību un brīvību būtība. Ievērojot proporcionalitātes principu, ierobežojumus drīkst uzlikt tikai tad, ja tie ir nepieciešami un patiešām atbilst vispārējas nozīmes mērķiem, ko atzinusi Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības."

Saskaņā ar minēto normu tiesību un brīvību izmantošanas ierobežojumiem ir jāatbilst pieciem kritērijiem, proti, tiem ir

1) jābūt noteiktiem tiesību aktos;
2) jārespektē tiesību un brīvību būtība;
3) jāatbilst vispārējas nozīmes mērķiem, ko atzinusi ES, vai vajadzībai aizsargāt citu personu tiesības un brīvības;
4) jābūt nepieciešamiem;
5) jābūt samērīgiem.

Hartā ietvertās tiesības atbilst ECTK garantētajām tiesībām, un šo tiesību nozīme un apjoms ir tāds pats kā ECTK noteiktajām tiesībām, kā to paredz Hartas 52. panta 3. punkts. Tajā pašā laikā minētā norma arī nosaka, ka tas neliedz ES tiesībās paredzēt plašāku aizsardzību. EST ir atzinusi, ka Hartas 52. panta 3. punkta mērķis ir nodrošināt nepieciešamo saskaņotību starp tajā ietvertajām tiesībām un atbilstošajām ECTK garantētajām tiesībām, tomēr negatīvi neietekmējot ES tiesību un EST autonomiju. Interpretējot Hartu, kā minimālās aizsardzības robeža ir jāņem vērā atbilstošās ECTK tiesības.[432] Cilvēktiesību ierobežošanas nosacījumi, kas paredzēti ECTK 8. panta 2. punktā, kā tos ir piemērojusi ECT, ir minimālie nosacījumi, kas jāievēro, ierobežojot Hartā paredzētās tiesības uz privātumu. Izvērtējot ES tiesību aktu atbilstību vai interpretāciju saskaņā ar Hartu,

431 European Court of Human Rights (2020), Guide on Article 8 of the Convention.

432 Sk. EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 124. punkts.

EST ir jāņem vērā garantijas, kuras noteiktas ECT praksē, izvērtējot atbilstību ECTK. Tajā pašā laikā EST var paredzēt arī plašāku aizsardzību.

Cilvēktiesību dokumentos paredzētie cilvēktiesību ierobežošanas kritēriji nosaka vispārējo kārtību, kādā ir jāveic samērīguma pārbaude un jāizvērtē tiesību ierobežošanas likumība, kas ir jāņem vērā, arī ieviešot jaunus masveida novērošanas pasākumus, to skaitā izmantojot jaunās tehnoloģijas. Eiropas Datu aizsardzības uzraudzītājs 2019. gadā publicēja Vadlīnijas par pasākumiem, kuri ierobežo pamattiesības uz privātumu un personas datu aizsardzību, proporcionalitātes novērtēšanu. Vadlīnijas balstās uz EST praksi masveida novērošanas lietās un skaidro proporcionalitātes principa piemērošanu. Vadlīnijas piedāvā praktisku metodiku jaunu likumdošanas pasākumu samērīguma novērtēšanai politikas veidotājiem un likumdevējam.[433] Dokumentā ir uzsvērts, ka nosacījumi iespējamiem pamattiesību ierobežojumiem ir vieni no svarīgākajiem Hartas elementiem, jo tie paredz, cik lielā mērā pamattiesības var tikt efektīvi izmantotas.[434] Tālāk apskatīts, kādus nosacījumus pamattiesību ierobežošanai ir noteikušas Eiropas pārnacionālās tiesas.

5.2. Nozīmīgākās masveida novērošanas lietas

ECT un EST ir izskatījusi un turpina izskatīt daudzas masveida novērošanas lietas.[435] ECT izskata sūdzības pret valstu novērošanas pasākumiem. Savukārt EST ir izskatījusi daudzas novērošanas lietas, kuras saistītas ar ES tiesību aktu spēkā esamību vai interpretāciju un kurās jautājumus ir uzdevusi valstu nacionālā tiesa, lūdzot sniegt prejudiciālo nolēmumu, vai arī ES institūcija, lūdzot sniegt viedokli. Daudzas nacionālās tiesas, kā arī Eiropas pārnacionālās tiesas izskata arī kolektīvās sūdzības masveida novērošanas lietās. Kā nodaļā atklāts, vairākas nevalstiskās organizācijas, piemēram, "Big Brother Watch", kā arī atsevišķas personas, piemēram, Maksimilians Šrems, kopējo interešu vārdā ir ierosinājušas stratēģiskās tiesvedības, lai apstrīdētu masveida novērošanas pasākumus.[436]

433 EDPS. (2019). EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en

434 Ibid.

435 Council of Europe. (2018). Mass surveillance; European Court of Human Rights (2020), Guide on Article 8 of the Convention, p. 40.

436 Taylor, van der Sloot, Floridi (2017), Conclusion: What Do We Know About Group Privacy?, pp. 232, 233.

5.2.1. Eiropas Cilvēktiesību tiesas prakse

ECT masveida novērošanas tiesu prakse ir ļoti plaša.[437] ECT ir izskatījusi daudzas uzraudzības lietas par elektronisko sakaru pārtveršanu[438], dažādiem novērošanas veidiem gan valsts, gan privātajā sektorā[439] un personas datu glabāšanu, ko veic valsts iestādes.[440] ECT ir atzinusi, ka ECTK 8. pants attiecas ne tikai uz valsts veiktu elektronisko sakaru novērošanu, bet arī, piemēram, uz videonovērošanu sabiedriskās vietās, piemēram, universitātēs un lielveikalos. Tālāk nodaļā apskatītas dažas nozīmīgākās ECT lietas.

Saskaņā ar ECT judikatūru tas būtu pretrunā ar valdību centieniem apkarot terorismu, ja terorisma draudi tiktu aizstāti ar iespējamiem draudiem no neierobežotas izpildvaras, kas iejaucas pilsoņu privātajā dzīvē.[441] Viena no pirmajām lietām, kurā ECT pieņēma spriedumu jau 1978. gadā, bija "Klāss u. c. pret Vāciju".[442] Šajā lietā iesniedzēji – pieci vācu juristi – apstrīdēja Vācijas tiesību aktus, kas pilnvaroja iestādes novērot viņu saraksti un telefona sakarus, neuzliekot tām pienākumu viņus vēlāk informēt par šiem pasākumiem. ECT nekonstatēja ECTK 8. panta pārkāpumu, atzīstot, ka iejaukšanās bijusi samērīga. Tajā pašā laikā tā pauda vairākas būtiskas atziņas. ECT atzina, ka ECTK 8. pantā noteiktais privātās dzīves jēdziens attiecas uz telefona sarunu slepenu noklausīšanos.[443] Tālāk tā norādīja, ka valsts likumdevējam ir zināma rīcības brīvība noteikt nosacījumus, saskaņā ar kuriem novērošanas sistēma darbojas. Tomēr tas nenozīmē, ka valstīm ir neierobežota rīcības brīvība pakļaut slepenai novērošanai to jurisdikcijā esošās personas. Apzinoties, ka šāds likums var radīt draudus demokrātijai vai pat to graut un iznīcināt, un izvirzot mērķi demokrātiju aizsargāt, valstis nedrīkst veikt jebkāda veida pasākumus, ko tās uzskata par piemērotiem cīņai pret spiegošanu un terorismu. Neatkarīgi no tā, kāda ir novērošanas sistēma, jāpastāv pietiekamām un efektīvām garantijām pret tās ļaunprātīgu izmantošanu. ECT norādīja, ka to izvērtējumam ir relatīvs raksturs, kas atkarīgs no visiem lietas apstākļiem, piemēram, iespējamo pasākumu rakstura, apjoma un ilguma, pamatojuma, kas

437 Sk. Council of Europe. (2018). Mass Surveillance; European Court of Human Rights (2020), Guide on Article 8 of the Convention.

438 Sk., piemēram, ECT 1984. gada 2. augusta spriedums lietā 8691/79 *Malone v. the United Kingdom*; ECT 2007. gada 3. aprīļa spriedums lietā 62617/00 *Copland v. The United Kingdom*; ECT 2017. gada 18. jūlija spriedums lietā 27473/06 *Mustafa Sezgin Tanrıkulu v Turkey*.

439 Sk., piemēram, ECT 1978. gada 6. septembra spriedums lietā 5029/71 *Klass and Others v. Germany*; ECT 2010. gada 2. septembra spriedums lietā *Uzun v. Germany*.

440 Sk., piemēram, ECT 2015. gada 4. decembra spriedums lietā 47143/06 *Roman Zakharov v. Russia*; ECT 2016. gada 12. janvāra spriedums lietā 37138/14.

441 Sk. Council of Europe (2018), Mass Surveillance.

442 ECT 1978. gada 6. septembra spriedums lietā 5029/71.

443 Turpat, 41. punkts.

nepieciešams šādu pasākumu ieviešanai, iestādes, kas ir kompetenta atļaut, veikt un uzraudzīt šādus pasākumus, valsts tiesību aktos paredzēto tiesiskās aizsardzības līdzekļu veida.[444]

ECT lietā "Szabó un Vissy pret Ungāriju" izvērtēja Ungārijas tiesību aktus, kas paredz slepenu, ar pretterorismu saistītu novērošanu, kas veikta, izmantojot jaunās tehnoloģijas, un ļauj masveidā pārtvert elektronisko sakaru datus. Iesniedzējs apgalvoja, ka regulējums nebija pietiekami detalizēts, precīzs, kā arī tas nesniedza pietiekamas garantijas pret datu ļaunprātīgu izmantošanu un valsts iestāžu patvaļu.[445]

ECT atgādināja, ka ECTK 8. pantā noteiktais privātās dzīves jēdziens attiecas uz sakaru un telefona sarunu noklausīšanos, ko veic policija, izlūkdienesti vai citas tiesībaizsardzības iestādes. Turklāt ECT spriedumā uzmanība tika vērsta arī uz to, ka, ņemot vērā slepenās novērošanas pasākumu īpatnības un to efektīvas kontroles un uzraudzības nozīmi, noteiktos apstākļos persona var apgalvot, ka ir upuris, tikai tāpēc, ka pastāv tiesību akti, kas atļauj slepenu novērošanu, pat ja šī persona nevar norādīt uz kādiem konkrētiem pasākumiem, kas viņu tieši ietekmē. [446]

ECT arī vērsa uzmanību, ka valdību iespēja iegūt detalizētu pilsoņu dzīves intīmāko aspektu aprakstu var radīt īpaši ierobežojošu iejaukšanos privātajā dzīvē.[447] Jāatceras, ka, izmantojot tehnoloģijas, kas balstītas uz mākslīgo intelektu, var daudz vieglāk veikt personas datu sasaisti dažādās sistēmās un profilu apvienošanu.[448]

ECT lietā arī norādīja, ka moderno tehnoloģiju, tostarp masveida komunikāciju novērošanas, izmantošana, lai novērstu potenciālus uzbrukumus, ir dabiskas sekas mūsdienu terorisma veidiem, ar ko valstīm nākas saskarties. Tomēr ECT atzina, ka attiecīgie Ungārijas tiesību akti nenodrošina pietiekamus aizsardzības pasākumus, lai izvairītos no ļaunprātīgas izmantošanas. ECT vērsa uzmanību, ka pasākumi varētu skart praktiski ikvienu Ungārijas iedzīvotāju, un jaunās tehnoloģijas ļauj valdībai viegli pārtvert liela apjoma datus, kas attiecas pat uz personām, attiecībā uz kurām šādas darbības sākotnēji netika paredzēts veikt. ECT konstatēja pārkāpumu, norādot, ka šādus pasākumus uzraudzīja tikai izpildvara, neizvērtējot, vai saziņas pārtveršana ir noteikti nepieciešama, un nepastāvēja neatkarīga tiesas kontrole un efektīvi tiesību aizsardzības pasākumi.

444 ECT 1978. gada 6. septembra spriedums lietā 5029/71, 49.–50. punkts.

445 ECT 2016. gada 12. janvāra spriedums lietā 37138/14, 33. punkts.

446 Turpat, 53. punkts.

447 Turpat, 70. punkts.

448 Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement, p. 38.

Grāmatas rakstīšanas laikā 2020. gada beigās ECT izskatīšanā atradās vairākas lietas par masveida komunikācijas datu novērošanu. 2019. gadā ECT paziņoja, ka tā atkārtoti izskatīs "Big Brother Watch u. c. pret Apvienoto Karalisti"[449] un "Centrum för Rättvisa pret Zviedriju"[450] lietas Lielajā palātā. 2018. gadā abās lietās ECT atzina, ka masveida novērošanas režīmi, lai gan aizskar tiesības uz privātumu, ir pieļaujami un paši par sevi nepārkāpj ECTK. Tāpat ECT uzsvēra, ka metadatu pārtveršana var būt tikpat aizskaroša, kā satura datu iegūšana. Tajā pašā laikā tā sniedza kritēriju sarakstu, kas jāņem vērā, izvērtējot pasākuma likumību, nepieciešamību un samērīgumu.

2018. gada 13. septembra spriedumā lietā "Big Brother Watch u. c. pret Apvienoto Karalisti" ECT konstatēja, ka Apvienotās Karalistes slepenās novērošanas programma pārkāpa ECTK 8. pantā noteiktās pamattiesības uz privātās dzīves ievērošanu nepietiekamas neatkarīgas uzraudzības un nepietiekamu aizsardzības pasākumu dēļ. Lieta attiecās uz žurnālistu un cilvēktiesību aizstāvju organizācijas sūdzību par trim dažādiem novērošanas režīmiem:

1) liela apjoma sakaru pārtveršanu;
2) sakaru datu iegūšanu, ko veica sakaru pakalpojumu sniedzēji, un
3) izlūkošanas informācijas apmaiņu ar ārvalstu valdībām.

ECT konstatēja pārkāpumus saistībā ar pirmajiem diviem gadījumiem. Tā vērsa uzmanību, ka pirmajā gadījumā nepastāvēja pietiekama uzraudzība pār pasākuma piemērošanu, bet otrajā gadījumā pasākums nebija skaidri noteikts likumā.[451] Šajā lietā ECT konstatēja, ka bija arī pārkāptas tiesības uz vārda brīvību, kas noteiktas ECTK 10. pantā, jo nepastāvēja pietiekami drošības pasākumi attiecībā uz konfidenciāliem žurnālistikas materiāliem.[452]

Savukārt 2018. gada 19. jūnija spriedumā lietā "Centrum för Rättvisa pret Zviedriju" ECT konstatēja, ka Zviedrijas lielapjoma sakaru pārtveršanas sistēma sniedz pietiekamas garantijas pret patvaļu un ļaunprātīgas izmantošanas risku. ECT norādīja šādus kritērijus, kas ļāva konstatēt pasākumu atbilstību: signālu izlūkošanas pasākumu darbības joma un pārtverto datu apstrāde bija skaidri noteikta likumā; atļaujai pārtvert datus vajadzēja būt ar tiesas lēmumu pēc detalizētas pārbaudes; pārtvert bija atļauts tikai sakarus, kas šķērso Zviedrijas robežu, bet ne pašā Zviedrijā; pārtveršana var ilgt tikai sešus mēnešus; jebkura atjaunošana prasīja pārskatīšanu; bija vairākas neatkarīgas struktūras, it īpaši Ārējās izlūkošanas inspekcija, kuras uzdevums bija uzraudzīt un pārskatīt sistēmu;

449 ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13, 62322/14, 24960/15 *Big Brother Watch and Others v. The United Kingdom.*

450 ECT 2018. gada 19. jūnija spriedums lietā 35252/08 *Centrum för Rättvisa v. Sweden.*

451 ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13 .., 387., 388. punkts.

452 Turpat, 495. punkts.

novērošanas pasākumu nepaziņošanu kompensēja fakts, ka bija pieejami vairāki sūdzību iesniegšanas mehānismi, it īpaši vēršoties pie Ārējās izlūkošanas inspekcijas, Parlamentārā ombuda un Tieslietu kanclera.[453]

ECT ir atzinusi, ka valstīm nav neierobežotas pilnvaras veikt iedzīvotāju masveida novērošanu. Saskaņā ar ECT praksi šāda novērošana ir pieļaujama tikai tad, ja tā ir absolūti nepieciešama demokrātisku mērķu aizsardzībai. Ņemot vērā lielo iespējamību, ka ECTK nostiprinātās pamattiesības uz privātumu un vārda brīvību var tikt pārkāptas, valstīm ir jānodrošina, ka, ieviešot novērošanas pasākumus, kas ietver masveida datu vākšanu, vienlaikus tiek izstrādāti arī tiesiski aizsardzības pasākumi, kas nodrošina cilvēktiesību ievērošanu.

Pamatkritērijiem, lai izvērtētu, vai masveida novērošanas pasākumi atbilst cilvēktiesībām, jābūt tikpat stingriem un saskaņotiem kā mērķtiecīgiem novērošanas pasākumiem.[454] Eiropas Padome ir norādījusi, ka ir ārkārtīgi svarīgi, lai valsts tiesību akti, kas atļauj aizskarošu novērošanas tehnoloģiju izmantošanu, paredz arī pietiekamas aizsardzības garantijas, lai novērstu vārda brīvības un tiesību uz privāto dzīvi riskus, kas rodas no milzīga datu apjoma masveida nediferencētas iegūšanas. Tāpēc ECT judikatūrā noteiktie standarti, kas saistīti ar mērķtiecīgu novērošanu, jāpielāgo arī masveida novērošanai.[455]

Lai gan ECT vēl nav skatījusi lietas par mākslīgā intelekta tehnoloģiju izmantošanas atbilstību cilvēktiesībām, tomēr tā ir paudusi viedokli par fotogrāfiju, kas glabājas policijas datubāzēs, izmantošanu sejas atpazīšanai. ECT 2020. gada 13. februārī pieņēma spriedumu lietā "Gaughran pret Apvienoto Karalisti" par notiesātas personas DNS profila, pirkstu nospiedumu un fotogrāfijas saglabāšanu.[456] Lietā cita starpā tika izskatīts jautājums par datubāzi, kurā glabātās fotogrāfijas var izmantot sejas atpazīšanas nolūkos, kas sākotnēji nebija iespējams, bet vēlāk kļuva iespējams, jo datus varēja pārsūtīt uz citu datubāzi, kuru varēja izmantot sejas atpazīšanai.[457] Proti, kopš 2016. gada jūlija Policijas nacionālajā datubāzē bija vairāk nekā 19 miljoni attēlu, no kuriem vairāk nekā 16 miljoni bija reģistrēti sejas atpazīšanas galerijā, padarot tos meklējamus, izmantojot sejas atpazīšanas programmatūru. ECT norādīja, ka iesniedzēja fotogrāfijas uzņemšana un saglabāšana nozīmē iejaukšanos viņa tiesībās uz privāto dzīvi ECTK 8. panta 1. punkta izpratnē, ņemot vērā to, ka fotogrāfija tika uzņemta viņa apcietināšanas laikā un

453 ECT 2018. gada 19. jūnija spriedums lietā 35252/08, 177., 178., 180. punkts.

454 Gstrein (2020), Mapping Power and Jurisdiction on the Internet ..

455 Council of Europe (2018), Mass Surveillance.

456 ECT 2020. gada 13. februāra spriedums lietā 45245/15 *Gaughran v. The United Kingdom.*

457 Turpat, 13., 37., 68., 69. punkts.

uz nenoteiktu laiku tiks glabāta vietējā datubāzē, lai to izmantotu policija, un ka policija var fotogrāfijai piemērot arī sejas atpazīšanu.[458]

ECT spriedumā nepārprotami tika noraidīts Apvienotās Karalistes valdības arguments – "jo vairāk dati tiek saglabāti, jo vairāk tiek novērsta noziedzība", norādot, ka "praksē šāda argumenta pieņemšana datu neierobežotas glabāšanas kontekstā būtu līdzvērtīga tam, ka tiktu atzīta par pieļaujamu informācijas glabāšana par visiem iedzīvotājiem un viņu mirušajiem radiniekiem, kas noteikti būtu pārmērīga un neatbilstoša".[459]

ECT arī vērsa uzmanību, ka ir jāizvērtē un jāpamato, kādos gadījumos un cik ilgu laiku dati ir jāglabā atkarībā, piemēram, no noziedzīgā nodarījuma smaguma, kā arī jānodrošina tiesību aizsardzības iespējas. ECT atzina, ka netiek nodrošināts līdzsvars starp konkurējošām valsts un personas interesēm, ņemot vērā prasītāja kā par pārkāpumu notiesātas personas (pat ja prasība tiek uzturēta) DNS profila, pirkstu nospiedumu un fotogrāfijas glabāšanas pilnvaru nediferencēto raksturu (šīs darbības veiktas neatkarīgi no nodarījuma smaguma vai nepieciešamības saglabāt datus nenoteiktu laiku) un reālu tiesību aizsardzības iespēju neesamību.

Visticamāk, šī lieta ir tikai sākums daudzām lietām, kuras nākotnē tiks iesniegtas par sejas atpazīšanas un citu mākslīgā intelekta sistēmu izmantošanu un kuras būs jāizskata gan ECT, gan EST.

5.2.2. Eiropas Savienības Tiesas prakse

EST daudzās lietās, kas saistītas ar masveida novērošanas pasākumiem, ir vērtējusi to atbilstību gan tiesībām uz privātumu, gan tiesībām uz datu aizsardzību. EST ir atzinusi, ka gadījumā, ja tiek ietekmētas Hartas 7. pantā noteiktās pamattiesības uz privātās dzīves neaizskaramību, apstrādājot personas datus, tiek ietekmētas arī tiesības uz datu aizsardzību, jo šāda apstrāde ietilpst Hartas 8. panta tvērumā un tai obligāti jāatbilst šajā pantā paredzētajām datu aizsardzības prasībām.[460] EST ir norādījusi, ka ES dalībvalstīm ar valsts tiesisko regulējumu noteiktais pienākums elektronisko komunikāciju pakalpojumu sniedzējiem saglabāt informāciju par datu plūsmu, lai to vajadzības gadījumā padarītu pieejamu kompetentajām valsts iestādēm, izraisa jautājumus ne tikai par privātās dzīves un personas datu aizsardzību, bet arī par Hartas 11. pantā garantēto vārda brīvību.

458 ECT 2020. gada 13. februāra spriedums lietā 45245/15 *Gaughran v. The United Kingdom*, 70. punkts

459 Turpat., 89. punkts.

460 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 170.–171. punkts.

Tas pats attiecas arī uz citiem datu apstrādes veidiem, piemēram, to nodošanu citām personām, kas nav lietotāji, vai piekļuvi šiem datiem, lai tos izmantotu.[461]

Personas datu izpaušana trešajai personai, piemēram, valsts iestādei, ir iejaukšanās Hartas 7. pantā un 8. pantā noteiktajās pamattiesībās, lai kāda būtu izpaustās informācijas tālākā izmantošana. Tas pats attiecas uz personas datu saglabāšanu, kā arī uz piekļuvi minētajiem datiem, lai valsts iestādes tos izmantotu neatkarīgi no tā, vai attiecīgajai informācijai par privāto dzīvi ir vai nav sensitīvs raksturs un vai ieinteresētajām personām ir vai nav radītas iespējamas neērtības šīs iejaukšanās dēļ.[462]

EST ir atzinusi – lai izpildītu samērīguma prasību, tiesiskajā regulējumā ir jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma tvērumu un piemērošanu un paredz minimālās prasības, lai tā rezultātā personām, kuru personas dati ir aizskarti, būtu pietiekamas garantijas, kas ļautu šos datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku. Tiesiskajā regulējumā it īpaši ir jānorāda, kādos apstākļos un ar kādiem nosacījumiem var īstenot pasākumus, kas ietver šādu datu apstrādi, tādējādi garantējot, ka iejaukšanās notiek tikai absolūti nepieciešamā robežās.[463] Līdz ar to valsts iestāžu piekļuve personas datiem, to saglabāšana un turpmāka izmantošana, īstenojot novērošanas pasākumus, nedrīkst pārsniegt robežas, kas ir absolūti nepieciešamas, citādi to "nevar uzskatīt par pamatotu demokrātiskā sabiedrībā".[464]

EST ir izskatījusi daudzas lietas, kas saistītas ar datu saglabāšanas pienākumu elektroniskās komunikācijas pakalpojumu sniedzējiem drošības iestāžu vajadzībām. Viena no būtiskajām lietām, kas īpaši nozīmīga privātuma un datu aizsardzības kā pamattiesību aizsardzības kontekstā, ir "Digital rights Ireland"[465] lieta, kurā EST pieņēma nolēmumu 2014. gadā. EST atzina šajā lietā par spēkā neesošu Datu saglabāšanas direktīvu, kas paredzēja elektroniskās komunikācijas pakalpojumu sniedzējiem pienākumu saglabāt datus un nodot tos drošības iestādēm pēc pieprasījuma. EST secināja, ka iejaukšanās pamattiesībās pārsniedz to, kas ir absolūti nepieciešams valsts drošības aizsardzībai, un tādējādi neatbilst Hartas 52. panta 1. punktā paredzētajam proporcionalitātes principam.

Pēc šī sprieduma EST izskatīja vēl vairākas lietas, kurās izvērtēja, vai ES tiesības pieļauj valstīs dažādus režīmus, kas paredz elektroniskās komunikācijas datu saglabāšanu nacionālajos tiesību aktos. 2016. gadā EST pieņēma nolēmumu

461 EST 2020. gada 6. oktobra spriedums lietā C-623/17 *Privacy International*, ECLI:EU:C:2020:790, 60.–61. punkts.

462 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 171. punkts.

463 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 68. punkts un tur minētā jurisprudence.

464 Turpat, 81. punkts.

465 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C293/12 ..

"Tele2 Sverige AB" un "Watson u. c."[466] apvienotajās lietās, atzīstot, ka E-privātuma direktīva neaizliedz dalībvalstīm pieņemt tiesību aktus, kas atvieglotu mērķtiecīgu (*targeted* – angļu val.) datu plūsmas un atrašanās vietas datu saglabāšanu smagu noziegumu apkarošanai, tajā pašā laikā tā aizliedz nacionālajās tiesībās paredzēt normas, kas uzliek elektronisko sakaru pakalpojumu sniedzējiem visaptverošu un nediferencētu datu saglabāšanas pienākumu.

Minētajā lietā EST arī atteicās no sava iepriekš paustā viedokļa, ka tiesību uz privātumu kontekstā komunikācijas saturs būtu vairāk aizsargājams nekā metadati. EST 2015. gada spriedumā "Schrems I" lietā norādīja, ka "it īpaši tiesiskais regulējums, saskaņā ar kuru valsts iestādēm vispārīgi tiek ļauts piekļūt elektronisko komunikāciju saturam, ir jāuzskata par tādu, kas apdraud pašu Hartas 7. pantā garantēto pamattiesību uz privātās dzīves neaizskaramību būtību".[467] Savukārt spriedumā "Tele 2 Sverige AB" un "Watson u. c." apvienotajās lietās, kā arī turpmākās lietās EST tomēr pamatoti atkāpās no šī apsvēruma, atzīstot, ka metadati kontekstā ar tiesībām uz privātās dzīves neaizskaramību var sniegt tikpat sensitīvu informāciju kā pats šīs komunikācijas saturs.[468] Dati, kuri tādējādi ir jāsaglabā elektronisko komunikāciju pakalpojumu sniedzējiem, ļauj atrast un identificēt saziņas avotu un tās adresātu, noteikt saziņas datumu, laiku, ilgumu un veidu, lietotāju izmantoto saziņas aparātu, kā arī noteikt mobilās saziņas aparāta atrašanās vietu. Šie dati ietver tostarp abonenta vai reģistrētā lietotāja vārdu un adresi, izsaucēja telefona numuru un zvana adresāta telefona numuru, kā arī IP adresi interneta pakalpojumiem. Šie dati it īpaši ļauj uzzināt, ar kuru personu abonents vai reģistrētais lietotājs ir sazinājies un kādu sakaru līdzekli viņš ir izmantojis, kā arī ļauj noteikt saziņas laiku un vietu, no kuras šī saziņa notikusi. Turklāt šie dati ļauj noskaidrot abonenta un reģistrēta lietotāja saziņas ar noteiktām personām biežumu noteiktā laikposmā.[469] Šie dati kopumā var ļaut izdarīt ļoti precīzus secinājumus par personu, kuru dati tikuši saglabāti, privāto dzīvi, proti, ikdienas paradumiem, pastāvīgajām vai pagaidu uzturēšanās vietām, ikdienas vai citām gaitām, veiktajām darbībām, šo personu sociālajiem kontaktiem un aprindām, kurās tās mēdz uzturēties. Šie dati sniedz iespējas noteikt attiecīgo personu profilu, kas kontekstā ar tiesībām uz privātās dzīves neaizskaramību ir tikpat sensitīva informācija kā pats šīs saziņas saturs.[470]

466 EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15 *Tele2 Sverige AB* un C-698/15 *Watson u. c.,* ECLI:EU:C:2016:970.

467 EST 2015. gada 6. oktobra spriedums lietā C-362/14, 94. punkts.

468 EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15 .., 98. punkts. Sk. arī EST 2014. gada 8. aprīļa spriedumu apvienotajās lietās C293/12 .., 26. punkts; EST 2020. gada 6. oktobra spriedumu apvienotajās lietās .., 117., 184. punkts.

469 EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15 .., 98. punkts.

470 Turpat, 99. punkts.

Vairākas ES dalībvalstis nepiekrita EST interpretācijai, ka ir aizliegta informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta glabāšana, jo uzskatīja, ka tām tiek atņemts būtisks instruments valsts drošības aizsargāšanai un cīņai pret terorismu. Šis pretējais viedoklis bija pamats vairākām jaunām EST prejudiciāla nolēmuma lūguma lietām par datu saglabāšanu, kurās apvienotais spriedums tika pasludināts 2020. gada 6. oktobrī – Francijas lietās C-511/18 "La Quadrature du Net u. c." un C-512/18 "French Data Network u. c." un Beļģijas lietā C-520/18 "Ordre des barreaux francophones et germanophone u. c."[471]

Atšķirībā no "Tele 2 Sverige AB" un "Watson u. c." lietām, kurās EST izvērtēja dalībvalstu regulējumu, kas paredzēja datu saglabāšanas pienākumu, lai apkarotu smagus noziegumus, jaunajās EST lietās jautājumi ir uzdoti par valsts drošības aizsardzību. EST tika jautāts, vai gadījumā, ja šādu pasākumu, kuri ierobežo tiesības uz privātumu un datu aizsardzību, mērķis ir valsts drošības garantēšana, interpretācija ir atšķirīga, t. i., vai E-privātuma direktīva ir piemērojama, un vai tomēr šādā gadījumā nebūtu pieļaujams paredzēt visaptverošu un nediferencētu datu saglabāšanas pienākumu.

Apvienotās Karalistes lietā "Privacy International" EST, atsaucoties uz savu iepriekšējo judikatūru, atgādināja, ka iejaukšanās Hartas 7. pantā paredzētajās tiesībās uz privātās dzīves neaizskaramību, ko rada informācijas par datu plūsmu un atrašanās vietas datu nodošana drošības dienestiem un izlūkdienestiem, ir jāuzskata par īpaši smagu, ņemot vērā tostarp informācijas, kuru var sniegt šie dati, sensitīvo raksturu un it īpaši iespēju, pamatojoties uz tiem, pierādīt datu subjekta profilu, jo šāda informācija ir tikpat sensitīva kā pats komunikācijas saturs. Turklāt šis apstāklis datu subjektu apziņā var radīt sajūtu, ka to privātā dzīve tiek pastāvīgi novērota.[472] Informācijas par datu plūsmu un atrašanās vietas datu nodošana valsts iestādēm drošības nolūkos pati par sevi var apdraudēt Hartas 7. pantā nostiprināto tiesību uz saziņas neaizskaramību. Tas elektroniskās komunikācijas līdzekļu izmantotājus var atturēt izmantot savu vārda brīvību, kas ir garantēta Hartas 11. pantā.[473] EST arī vērsa uzmanību, ka, ņemot vērā informācijas par datu plūsmu un atrašanās vietas datu, kurus var pastāvīgi saglabāt ar visaptverošu un nediferencētu saglabāšanas pasākumu, ievērojamo apjomu, kā arī informācijas, ko šie dati var sniegt, sensitīvo raksturu, pati minēto datu saglabāšana, ko veic elektronisko komunikāciju pakalpojumu sniedzēji, ietver ļaunprātīgas izmantošanas un

471 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 ..

472 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 71. punkts. Sk. arī EST 2014. gada 8. aprīļa spriedumu apvienotajās lietās C-293/12 **..**, 27. un 37. punkts, kā arī EST 2016. gada 21. decembra spriedumu apvienotajās lietās C-203/15 .., 99. un 100. punkts.

473 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 72. punkts.

prettiesiskas piekļuves risku.[474] Lai izpildītu samērīguma prasību, atkāpes no personas datu aizsardzības un tās ierobežojumi ir jāīsteno absolūti nepieciešamā robežās. Vispārēja piekļuve visiem saglabātajiem datiem, kas nav atkarīga no jebkādas, kaut arī netiešas, saiknes ar sasniedzamo mērķi, nevar tikt uzskatīta par tādu, kas ir absolūti nepieciešama.[475] Tā kā informācijas par datu plūsmu un atrašanās vietas datu nodošana notiek visaptveroši un nediferencēti, tā vispārīgi attiecas uz visām personām, kas izmanto elektronisko komunikāciju pakalpojumus. Tādējādi valsts iestādes saglabā un nodod datus pat par tām personām, par kurām nav nekādu norāžu, kas ļautu uzskatīt, ka to rīcība varētu apdraudēt (pat netieši vai attāli) valsts drošības intereses, un it īpaši netiek pierādīta saikne starp datiem, kuru nodošana ir paredzēta, un draudiem valsts drošībai.[476] EST atzina, ka tāds valsts tiesiskais regulējums, saskaņā ar kuru valsts iestādei valsts drošības aizsardzības nolūkā ir atļauts elektronisko komunikāciju pakalpojumu sniedzējiem noteikt pienākumu veikt visaptverošu un nediferencētu informācijas par datu plūsmu un atrašanās vietas datu nodošanu drošības dienestiem un izlūkdienestiem, pārsniedz absolūti nepieciešamā robežas un ir pretrunā Hartas 7., 8. un 11. pantam.[477]

EST spriedumā lietā "La Quadrature du Net u. c." vispirms līdzīgi atzina, ka tādi tiesību akti, ar kuriem preventīvi paredzēta informācijas par datu plūsmu, kā arī atrašanās vietas datu visaptveroša un nediferencēta saglabāšana valsts un sabiedrības drošības un aizsardzības mērķu vārdā, nav pretrunā ar ES tiesībām. Situācijās, ja pastāv nopietni draudi valsts drošībai, "kuri izrādās patiesi un faktiski vai paredzami", ir pieļaujama visaptveroša un nediferencēta informācijas par datu plūsmu, kā arī atrašanās vietas datu saglabāšana un nodošana. Tādējādi EST atzina, ka izņēmuma gadījumā ir pieļaujama masveida datu – tālruņu un interneta lietotāju personas datu – saglabāšana un nodošana drošības dienestiem arī preventīvos nolūkos, ja pastāv nopietni draudi valsts drošībai. Tāpat EST norādīja, ka saglabāšanai vajadzētu būt ierobežotai laikā, un tas ir absolūti nepieciešams, kā arī ir jāievieš efektīvas garantijas un neatkarīgs pārskatīšanas mehānisms.[478]

EST arī norādīja – lai aizsargātu valsts drošību, apkarotu smagus noziegumus un novērstu nopietnus draudus sabiedrības drošībai, var tikt veikta informācijas par datu plūsmu un atrašanās vietas datu mērķorientēta saglabāšana, kura, pamatojoties uz objektīviem un nediskriminējošiem elementiem, tiek ierobežota atkarībā no attiecīgo personu kategorijām vai pamatojoties uz ģeogrāfisku kritēriju uz laiku, kas nepārsniedz absolūti nepieciešamo, kuru tomēr var pagarināt.

474 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 73. punkts.

475 Turpat, 78. punkts.

476 Turpat, 80. punkts.

477 Turpat, 81. punkts.

478 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 177., 192. punkts.

Tāpat, lai sasniegtu minētos mērķus, ir atļauta arī visaptveroša un nediferencēta elektronisko sakaru līdzekļu lietotāju identitātes datu un savienojuma avotam piešķirtās IP adreses saglabāšana uz laiku, kas nepārsniedz absolūti nepieciešamo.

EST arī atzina, ka ir pieļaujama datu vākšana un analīze reāllaikā. Proti, elektronisko sakaru pakalpojumu sniedzējiem var noteikt pienākumu automatizēti reāllaikā analizēt un vākt informāciju par datu plūsmu un atrašanās vietas datiem, kā arī par tehniskajiem datiem, kas savākti par gala iekārtu izmantošanu. Šādu automatizētu analīzi var izmantot tikai situācijās, kad valsts saskaras ar nopietniem draudiem valsts drošībai, kas izrādās patiesi un faktiski vai paredzami. Savukārt informāciju par datu plūsmu un atrašanās vietas datus reāllaikā var vākt tikai tad, ja tā attiecas uz personām, attiecībā uz kurām ir pamatots iemesls aizdomām, ka tās kaut kādā veidā ir iesaistītas terorisma darbībās.[479]

EST ar spriedumu "La Quadrature du Net u. c." lietā būtībā akceptē visaptverošu un nediferencētu datu saglabāšanu, lai gan tikai izņēmuma gadījumos un tikai tad, ja tas ir stingri nepieciešams demokrātiskā sabiedrībā un samērīgs ar paredzamo nolūku, turklāt tiek pieprasīts ieviest stingras aizsardzības garantijas. Tādējādi EST pietuvinās ECT pieejai, kas līdzīgi atzīst masveida datu saglabāšanu par pieļaujamu, ja vien tiek ievēroti ierobežošanas kritēriji un aizsardzības garantijas.

Apskatītais EST spriedums krasi kontrastē ar spriedumu lietā C-311/18 "Schrems II", kas tika pieņemts dažus mēnešus iepriekš. EST ar minēto spiedumu otro reizi atzina par spēkā neesošu ES un ASV datu nodošanas līgumu, ņemot vērā ASV pastāvošo novērošanas režīmu. Proti, EST gan 2015. gada spriedumā "Schrems I" lietā, gan 2020. gada jūlija spriedumā "Schrems II" lietā konstatēja, ka Eiropas Komisijas lēmumi par aizsardzības līmeņa pietiekamību datu nodošanai uz ASV, kas veidoja pamatu datu nodošanai no ES uz ASV, ir spēkā neesoši. EST ES un ASV privātuma vairoga atzīšana par spēkā neesošu bija balstīta uz vairākiem faktoriem. Tie ir šādi:

1) ASV tiesībaizsardzības prasību prioritāte pār privātuma vairoga prasībām;[480]
2) nepieciešamo varas pilnvaru ierobežojumu un garantiju trūkums saskaņā ar ASV tiesību aktiem, it īpaši, ņemot vērā proporcionalitātes prasības;[481]
3) efektīvs tiesību aizsardzības līdzekļu trūkums ASV ES datu subjektiem[482] un
4) trūkumi privātuma vairoga ombuda mehānismā.[483]

479 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 192. punkts.

480 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 164. punkts.

481 Turpat, 168.–185. punkts.

482 Turpat, 191.–192. punkts.

483 Turpat, 193.–197. punkts. Sk. vairāk Kuner, C. (17 July, 2020). The Schrems II judgment of the Court of Justice and the future of data transfer regulation. *European Law Blog.* https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

EST noraidīja Eiropas Komisijas skaidrojumu, ka ASV valsts iestāžu iejaukšanās to personu pamattiesībās, kuru dati privātuma vairoga ietvaros no ES tiek nosūtīti uz ASV, ja tas notiek valsts drošības, tiesībaizsardzības vai citu valsts interešu nolūkos, un sekojošie ierobežojumi, kas noteikti pašsertificētām organizācijām attiecībā uz to principialitāti, būs ierobežoti līdz tādam apmēram, kas ir absolūti nepieciešams, lai sasniegtu attiecīgo likumīgo mērķi, un tādējādi tie nodrošina efektīvu tiesisko aizsardzību pret šādu iejaukšanos. EST gluži pretēji secināja, ka tiesību normas, uz kurām ir balstīta novērošanas programma, neatbilst minimālajām prasībām, kas ES tiesībās izriet no samērīguma principa, un nevar uzskatīt, ka tās ir ierobežotas līdz absolūti nepieciešamajam.[484] EST secināja, ka privātuma vairogs nenodrošina aizsardzību, kas ir līdzvērtīga Hartā noteiktajām pamattiesībām, jo datiem, kas pārsūtīti saskaņā ar minēto lēmumu, ASV iestādes varēja piekļūt un tos turpmāk apstrādāt, pārsniedzot to, kas ir stingri nepieciešams un samērīgs ar valsts drošības aizsardzības nolūku. "Schrems II" spriedums pieprasa ņemt vērā divas specifiskas prasības: pirmkārt, spriedums nosaka nepieciešamību pēc tiesiskās aizsardzības līdzekļiem, proti, ir jāparedz efektīvas un izpildāmas individuālas pārsūdzības tiesības neatkarīgas un objektīvas tiesas priekšā[485], un, otrkārt, attiecībā uz noteiktu novērošanas programmu apjomu – ir jāparedz ierobežojumi valsts iestāžu piekļuvei personas datiem, lai netiktu pārkāpts absolūtas nepieciešamības un proporcionalitātes princips.[486]

ES un ASV privātuma vairogs nav vienīgais datu nodošanas līgums, ko EST ir atzinusi par spēkā neesošu. 2017. gadā EST pieņēma Atzinumu 1/15 par Nolīguma projektu starp Kanādu un ES par pasažieru datu reģistra datu pārsūtīšanu no ES uz Kanādu. EST paziņoja, ka nolīgumu nevar noslēgt tā pašreizējā formā, jo vairāki tā noteikumi nav savienojami ar tiesībām uz privātumu un datu aizsardzību. Lai gan nolīgumam ir leģitīms mērķis, t. i., sabiedrības drošība un terorisma apkarošana, vairāki tā noteikumi neaprobežojas tikai ar to, kas ir absolūti nepieciešams, un tajā nav paredzēti skaidri un precīzi noteikumi, piemēram, par sensitīvu datu apstrādi. EST atzina, ka visu aviopasažieru datu turpmāka glabāšana pēc pasažieru izlidošanas neaprobežojās tikai ar to, kas ir absolūti nepieciešams, un tā būtu jāattiecina tikai uz tiem pasažieriem, kuru gadījumā ir objektīvas pazīmes, kas liecina, ka viņi varētu radīt risku saistībā ar cīņu pret terorismu un smagiem starptautiskiem noziegumiem. 2020. gada martā Vācijas tiesa uzdeva EST prejudiciālo jautājumu, vai pamattiesībām atbilst Eiropas pasažieru datu saglabāšanas

484 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 167., 184. punkts.

485 Turpat, 167., 184. punkts.

486 Turpat, 179., 180., 183., 185. punkts.

direktīva, kas ļauj iestādēm analizēt un uzglabāt to cilvēku personas datus, kuri veic starptautiskos lidojumus Eiropā.[487]

Gan EST, gan ECT turpina izskatīt lietas par liela apjoma datu saglabāšanu, nodošanu un novērošanu drošības nolūkos. Sagaidāms, ka nākotnē tām būs jāizskata arī lietas par mākslīgā intelekta tehnoloģiju izmantošanas atbilstību cilvēktiesībām. Tajā pašā laikā jau šobrīd judikatūrā izstrādātās būtiskās garantijas ir attiecināmas arī uz jauniem masveida datu vākšanas un novērošanas pasākumiem, to skaitā tādiem, kas izmanto mākslīgā intelekta tehnoloģijas.

5.3. Būtiskās garantijas novērošanas pasākumiem

No abu Eiropas pārnacionālo tiesu judikatūras ir identificējamas vairākas būtiskas garantijas, kas jāievēro, lai nodrošinātu, ka tiesību uz privātumu un datu aizsardzību ierobežošana, piemērojot novērošanas pasākumus, ir proporcionāla un nepieciešama demokrātiskā sabiedrībā.

EST praksē ir plaši vērtēts, vai indivīdu tiesību ierobežojumi atbilst 52. panta nosacījumiem un it īpaši – vai tie ir noteikti tiesību aktos un vai ir samērīgi un nepieciešami demokrātiskā sabiedrībā. EST uzsver arī neatkarīgas iestādes kontroles nozīmi, kas paredzēta Hartas 8. panta 3. punktā, kā arī efektīvu tiesību aizsardzības līdzekļu nozīmi, kas ir noteikti Hartas 47. pantā. Līdzīgi arī ECT praksē ir atzīts, ka indivīdu tiesību ierobežojumam ir jābūt noteiktam ar likumu, tam ir jābūt samērīgam un nepieciešamam demokrātiskā sabiedrībā, kā arī ir jābūt efektīviem tiesību aizsardzības līdzekļiem, ko var izmantot aizskartās personas. Eiropas Datu aizsardzības kolēģija 2020. gada novembrī publicēja Ieteikumus 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem, kura tika izstrādāta pēc EST "Schrems II" sprieduma pieņemšanas. Tā tika sagatavota, balstoties uz iepriekš 2016. gadā 29. panta darba grupas izstrādāto dokumentu 01/2016 par pamatojumu pamattiesību uz privātumu un datu aizsardzību ierobežošanai, izmantojot novērošanas pasākumus personas datu nosūtīšanas gadījumā[488], un kurš savukārt tika publicēts pēc EST "Schrems I" sprieduma. Abos dokuments ir norādīts, ka tiesiskās prasības, kuras izriet no EST un ECT judikatūras masveida novērošanas lietās un kuras ir jāievēro, lai privātuma un datu

487 Lūgums sniegt prejudiciālu nolēmumu, ko 2020. gada 27. maijā iesniedza *Verwaltungsgericht Wiesbaden* (Vācija) – OC/*Bundesrepublik Deutschland*, EST lieta C-148/20, ES OV, C 279/30, 24.08.2020.

488 Article 29 Data Protection Working Party. (2016). Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees). https://ec.europa.eu/newsroom/article29/items/640363/en

aizsardzības ierobežojumi varētu tikt uzskatīti par attaisnojamiem saskaņā ar Hartu, var apkopot četrās būtiskās garantijās:

1) apstrādei jābalstās uz skaidru, precīzu un pieejamu regulējumu;
2) ir jāpierāda nepieciešamība un samērīgums attiecībā uz izvirzītajiem likumīgajiem mērķiem;
3) jāpastāv neatkarīgam uzraudzības mehānismam;
4) personām ir jābūt pieejamiem efektīviem tiesību aizsardzības līdzekļiem.[489]

Nodaļas turpinājumā konkrētāk aplūkots, ko paredz katra no šīm būtiskajām garantijām.

5.3.1. Skaidrs, precīzs un pieejams regulējums

Pirmais nosacījums, kas ir jāpārbauda, kad ir konstatēts, ka pastāv iejaukšanās tiesībās uz datu aizsardzību, ir – vai šāda iejaukšanās ir "paredzēta likumā".

Minētā prasība ir ietverta Hartas 52. panta 1. punktā, kas nosaka, ka visiem Hartā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jābūt paredzētiem tiesību aktos. Turklāt Hartas 8. panta 2. punkts paredz personas datu apstrādes nosacījumus, proti, ka šādi dati ir jāapstrādā godprātīgi, noteiktiem mērķiem un ar likumīgu pamatojumu, kas paredzēts tiesību aktos.

Hartā noteiktā prasība, saskaņā ar kuru jebkuram pamattiesību ierobežojumam ir jābūt noteiktam tiesību aktos, nozīmē, ka pašā juridiskajā pamatā ir jānosaka attiecīgo tiesību īstenošanas ierobežojuma apjoms. Juridiskajā pamatā, kas ļauj iejaukties pamattiesībās, lai tas atbilstu samērīguma principam, ir arī jāparedz skaidri un precīzi noteikumi attiecībā uz konkrētā pasākuma tvērumu un piemērošanu, kā arī minimālās aizsardzības garantijas.[490] EST turklāt atgādina, ka personām garantētajām tiesībām ir jābūt efektīvām un īstenojamām.

EST "Schrems II" lietā konstatēja, ka no attiecīgā ASV tiesiskā regulējuma neizriet ne tas, ka pastāv pilnvaru ierobežojumi novērošanas programmu īstenošanai ārējās izlūkošanas mērķiem, ne arī garantijas personām, kuras nav ASV pilsoņi un kuras potenciāli skar šīs programmas, tādējādi nevar tikt nodrošināts tāds aizsardzības līmenis, kas būtībā būtu līdzvērtīgs Hartā garantētajam. Tāpat tā konstatēja, ka datu subjektiem, kuru dati ir pārsūtīti uz attiecīgo trešo valsti, nav piešķirtas tiesības, kuras viņi tiesās varētu īstenot pret ASV iestādēm. Līdz ar to privātuma vairogs, pretēji tam, kas noteikts VDAR 45. panta 2. punkta

489 Eiropas Datu aizsardzības kolēģija. (2020). Ieteikumi 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_lv

490 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 175., 180., 181. punkts; EST 2017. gada 26. jūlija atzinums 1/15 *Accord PNR UE-Canada*, ECLI:EU:C:2017:592, 139. punkts un tajā minētā judikatūra.

a) apakšpunktā, nevar nodrošināt būtībā līdzvērtīgu aizsardzības līmeni tam, kāds izriet no Hartas.[491]

EST lietā "Privacy International" līdzīgi norādīja – lai izpildītu samērīguma prasību, tiesiskajā regulējumā ir jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma tvērumu un piemērošanu un paredz minimālās prasības, lai tā rezultātā personām, kuru personas dati tikuši pārsūtīti, būtu pietiekamas garantijas, kas ļautu šos datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku. Šim tiesiskajam regulējumam ir jābūt juridiski saistošam valsts tiesībās, un tajā it īpaši ir jānorāda, kādos apstākļos un ar kādiem nosacījumiem var īstenot pasākumu, kas ietver šādu datu apstrādi, tādējādi garantējot, ka šāda iejaukšanās notiek tikai absolūti nepieciešamās robežās. Šādu garantiju sniegšanas nepieciešamība ir vēl jo svarīgāka tādēļ, ka personas dati tiek apstrādāti automātiski un pastāv ievērojams nelikumīgas piekļuves risks šiem datiem. Šie apsvērumi ir it īpaši svarīgi, ja runa ir par tādas kategorijas personas datu aizsardzību kā sensitīvi dati.[492]

ECT ir vērsusi uzmanību – nosacījums, ka pamattiesību ierobežošanai ir jābūt "paredzētai likumā", nozīmē: novērošanas pasākumam ir jābūt zināmam pamatam nacionālajā likumdošanā un tam jāatbilst tiesiskuma principam.[493] ECT judikatūrā ir noteiktas sešas minimālās aizsardzības garantijas, kas ir jāparedz tiesiskajā regulējumā attiecībā uz slepenu novērošanas pasākumu piemērošanu, lai izvairītos no varas ļaunprātīgas izmantošanas:

1) nodarījumu jeb pārkāpumu veids, kas var izraisīt noklausīšanās rīkojumu;
2) to cilvēku kategorijas, kuru tālruņus var noklausīties;
3) telefona sarunu noklausīšanās ilguma ierobežojums;
4) kārtība, kas jāievēro, pārbaudot, izmantojot un uzglabājot iegūtos datus;
5) piesardzības pasākumi, kas jāievēro, paziņojot datus citām pusēm;
6) apstākļi, kādos ierakstus var vai ir nepieciešams izdzēst vai iznīcināt.[494]

491 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 180., 181. punkts.

492 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 68. punkts un tajā minētā judikatūra. Sk. arī EST 2014. gada 8. aprīļa spriedumu apvienotajās lietās C293/12 .., 55. punkts; EST 2016. gada 21. februāra spriedumu apvienotajās lietās C-203/15 .., 117. punkts; EST 2017. gada 26. jūlija atzinums 1/15, 141. punkts.

493 European Court of Human Rights (2020), Guide on Article 8 of the Convention, p. 124.

494 ECT 2016. gada 12. janvāra spriedums lietā 37138/14, 56. punkts; ECT 2015. gada 4. decembra spriedums lietā 47143/06, 231., 238.–301. punkts; ECT 2000. gada 16. februāra spriedums lietā 27798/95 *Amann v. Switzerland*, 56.–58. punkts.

Likumā ir jānorāda arī izpildvarai vai tiesnesim piešķirtās rīcības brīvības apjoms un tā izmantošanas veids ar pietiekamu skaidrību, lai indivīdam nodrošinātu pietiekamu aizsardzību pret patvaļīgu iejaukšanos.[495]

Viens no galvenajiem nosacījumiem, ko ir uzsvērusi ECT, – likumam jābūt pieejamam attiecīgajai personai un paredzamam attiecībā uz tā sekām.[496] Sakaru pārtveršanas kontekstā "paredzamību" nevar saprast tāpat kā daudzās citās jomās. Paredzamība slepenu novērošanas pasākumu kontekstā nenozīmē, ka indivīdiem jāspēj paredzēt, kad iestādes, iespējams, pārtver viņu saziņu, lai viņi varētu attiecīgi pielāgot savu rīcību.[497] Tomēr, lai izvairītos no patvaļīgas iejaukšanās, ir svarīgi, lai būtu skaidri, detalizēti noteikumi par tālruņa sarunu pārtveršanu. Likumam jābūt pietiekami skaidram, lai iedzīvotājiem sniegtu atbilstošu norādi par apstākļiem un nosacījumiem, kādos valsts iestādes ir pilnvarotas izmantot šādus slepenus pasākumus.[498]

Šajā ziņā pasākumiem jābūt paredzamiem un pieejamiem personām, kuras arī ir jāinformē par valsts iestāžu iespējamo piekļuvi datiem, ko šīs personas sniedz privātiem uzņēmumiem, lai saņemtu pakalpojumu, piemēram, rezervējot lidojumu, pārskaitot naudu, nosūtot e-pastu vai īsziņu vai pārlūkojot internetu. Novērošanas programmas, kas gadiem ilgi darbojas slepeni un ko atklāja plašsaziņas līdzekļi vai trauksmes cēlēji, piemēram, PRISM, neatbilst šīm prasībām.[499]

Nosacījums, ka ierobežojumiem ir jābūt skaidri un precīzi noteiktiem tiesiskajā regulējumā, ir attiecināms arī uz valsts iestāžu novērošanas pasākumiem, kas balstās uz jaunajām tehnoloģijām, tostarp sejas atpazīšanas tehnoloģijām. Šādus pasākumus nevar īstenot slepeni, tos skaidri nenosakot tiesību aktos. Tiesiskajā regulējumā ir jāparedz, kādi ir to piemērošanas apstākļi un nosacījumi, kādas personas tas skar, kādas aizsardzības garantijas tiek piemērotas, kā arī kādas ir personu iespējas efektīvi aizsargāt savas tiesības. Prasības pēc atbilstoša tiesiskā regulējuma izriet arī no datu aizsardzības prasībām (tas atklāts grāmatas

495 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 230. punkts; ECT 1984. gada 2. augusta spriedums lietā 8691/79, 68. punkts; ECT 1990. gada 24. aprīļa spriedums lietā 11105/84 *Huvig v. France,* 29. punkts; ECT 2006. gada 29. jūnija lēmums lietā 54934/00 *Weber and Saravia v. Germany*, 94. punkts.

496 ECT 2010. gada 18. maija spriedums lietā 26839/05 *Kennedy v. the United Kingdom*, 151. punkts; ECT 2015. gada 4. decembra spriedums lietā 47143/06, 229. punkts.

497 ECT 2006. gada 29. jūnija lēmums lietā 54934/00, 93. punkts.

498 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 229. punkts; ECT 2007. gada 28. jūnija spriedums lietā *The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 75. punkts; ECT 2018. gada 13. septembra spriedums .. 58170/13, 62322/14, 24960/15, 307. punkts.

499 Tzanou (2019), *The Fundamental Right to Data Protection*, p. 253.

sestajā nodaļā), tajā pašā laikā tās tiešā veidā izriet arī no prasības, ka cilvēktiesību ierobežojumiem ir jābūt noteiktiem tiesību aktā.

Tomēr tas vien, ka ierobežojumi ir noteikti tiesību aktā, vēl nenozīmē, ka tie ir likumīgi. Nākamais nosacījums, kas jāpārbauda, ir samērīgums un nepieciešamība.

5.3.2. Samērīgums un nepieciešamība

Hartas 52. panta 1. punkta pirmais teikums paredz, ka visiem Hartā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jārespektē šo tiesību un brīvību būtība. Tālāk minētās normas otrais teikums paredz, ka, ievērojot proporcionalitātes principu, ierobežojumus drīkst uzlikt tikai tad, ja tie ir nepieciešami un patiešām atbilst vispārējas nozīmes mērķiem, ko atzinusi ES, vai vajadzībai aizsargāt citu personu tiesības un brīvības.

Satversmes tiesa, izvērtējot pamattiesību ierobežojumu samērīgumu, pārbauda trīs aspektus:

1) vai izraudzītie līdzekļi ir piemēroti leģitīmā mērķa sasniegšanai, proti, vai ar izraudzīto līdzekli var sasniegt leģitīmo mērķi;
2) vai šāda rīcība ir nepieciešama, proti, vai leģitīmo mērķi nevar sasniegt ar indivīda tiesības mazāk ierobežojošiem līdzekļiem;
3) vai ierobežojums ir atbilstošs, proti, vai labums, ko iegūst sabiedrība, ir lielāks par indivīda tiesībām nodarīto kaitējumu.

Ja tiek atzīts, ka pamattiesību ierobežojums neatbilst kaut vienam no šiem kritērijiem, tad tas neatbilst samērīguma principam un ir prettiesisks.[500] Attiecībā uz pirmo nosacījumu – likumdevēja izraudzītie līdzekļi ir piemēroti leģitīmā mērķa sasniegšanai, ja ar konkrēto regulējumu šis mērķis tiek sasniegts.[501] Attiecībā uz otro nosacījumu – pamattiesību ierobežojums ir nepieciešams, ja nepastāv citi līdzekļi, kuri būtu tikpat iedarbīgi un kurus izvēloties personu pamattiesības tiktu ierobežotas mazāk.[502]

EST izmanto līdzīgu pieeju, lai izvērtētu samērīguma principa ievērošanu. Turklāt saskaņā ar tās pastāvīgo judikatūru atkāpes un ierobežojumi personas datu aizsardzībai ir jāpiemēro tikai tiktāl, ciktāl tas ir "absolūti nepieciešams".

EST spriedumā apvienotajās lietās "Digital rights Ireland" un "Seitlinger u. c." norāda, ka atbilstoši samērīguma principam ES iestāžu tiesību aktiem ir jābūt piemērotiem attiecīgajā tiesiskajā regulējumā noteikto leģitīmo mērķu sasniegšanai

500 Sk., piemēram, Satversmes tiesas 2020. gada 18. novembra spriedums lietā Nr. 2019-32-01, 16. punkts.

501 Turpat, 17. punkts.

502 Turpat, 18. punkts.

un tie nedrīkst pārsniegt to, kas ir to sasniegšanai atbilstošs un nepieciešams.[503] ES likumdevēja novērtējuma brīvība var būt ierobežota atkarībā no daudziem faktoriem, tostarp no skartās jomas, attiecīgo Hartā garantēto tiesību rakstura, iejaukšanās rakstura un būtiskuma, kā arī tās mērķa.[504] Tajā pašā laikā tiesību uz privātās dzīves neaizskaramību aizsardzība katrā ziņā prasa, lai atkāpes no personas datu aizsardzības un tās ierobežojumi tiktu īstenoti "absolūti nepieciešamā" ietvaros.[505] Minētajā lietā EST atzina, ka Datu saglabāšanas direktīva ES tiesību sistēmā rada plaša apjoma un īpaši būtisku iejaukšanos Hartas 7. un 8. pantā garantētajās pamattiesībās un šī iejaukšanās nav precīzi reglamentēta ar tiesību normām, kas ļautu nodrošināt, lai tā patiešām būtu ierobežota ar "absolūti nepieciešamo".

Arī attiecībā uz ES dalībvalstu tiesību aktiem EST lietā "Privacy International" atzina, ka valsts tiesiskais regulējums, kas valsts iestādei valsts drošības aizsardzības nolūkā atļauj elektronisko komunikāciju pakalpojumu sniedzējiem noteikt pienākumu veikt visaptverošu un nediferencētu informācijas par datu plūsmu un atrašanās vietas datu nodošanu drošības dienestiem un izlūkdienestiem, pārsniedz absolūti nepieciešamā robežas.[506]

EST ir norādījusi, ka dalībvalstu piemērotie tiesību ierobežojumi ir jāizvērtē, izsverot iejaukšanās, ko rada šāds ierobežojums, smagumu, un pārbaudot, vai vispārējo interešu mērķa nozīmīgums, kas ir šī ierobežojuma pamats, ir atbilstošs šim smagumam.[507]

EST spriedumā lietā "La Quadrature du Net u. c.", atsaucoties uz tās pastāvīgo judikatūru, atkārtoti uzsver, ka pamattiesību uz privātās dzīves neaizskaramību aizsardzība atbilstoši tās pastāvīgajai judikatūrai nozīmē, ka atkāpes no personas datu aizsardzības un tās ierobežojumi ir jāīsteno, ja tas ir "absolūti nepieciešams". Turklāt vispārējo interešu mērķi nevar sasniegt, neņemot vērā to, ka tas ir jāsaskaņo ar pamattiesībām, uz kurām attiecas pasākums, līdzsvarojot vispārējo interešu mērķi, no vienas puses, ar attiecīgajām tiesībām, no otras puses.[508]

Izvērtējot valstu masveida novērošanas pasākumu likumību, EST un ECT judikatūrā pamatā tiek samērotas personas tiesības uz privātumu un datu aizsardzību, no vienas puses, ar valsts drošības, sabiedrības drošības un noziedzības apkarošanas interesēm, no otras puses. EST lietā "La Quadrature du Net u. c.", kas

503 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C293/12 .., 46. punkts.

504 Turpat, 47. punkts.

505 Turpat, 52. punkts.

506 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 81. punkts.

507 Turpat, 131. punkts.

508 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 130. punkts; EST 2020. gada 6. oktobra spriedums lietā C-623/17, 68. punkts

saistīta ar dalībvalsts tiesību aktiem, nolēma, ka valsts drošības aizsardzības mērķis tā svarīguma dēļ spēj attaisnot pasākumus, kas rada būtiskāku pamattiesību aizskārumu, bet ne pasākumus, kurus varētu pamatot ar citiem mērķiem, piemēram, noziedzības apkarošanu. Tomēr tā konstatēja, ka tas tā ir, ja ir pietiekami nopietni iemesli uzskatīt, ka attiecīgā valsts saskaras ar nopietniem draudiem valsts drošībai, kas ir pierādīti kā patiesi un faktiski vai paredzami un ir pakļauti citu Hartas 52. panta 1. punktā noteikto prasību izpildei.[509]

Jautājums, vai ierobežojumi ir samērīgi un nepieciešami, ir izvērtējams kopsakarā ar pirmo, iepriekš aplūkoto nosacījumu, t. i., kādā veidā ierobežojumi ir paredzēti tiesību aktā. EST "Schrems II" lietā norāda – lai izpildītu samērīguma prasību, attiecīgajā tiesiskajā regulējumā, kas paredz datu aizsardzības ierobežojumus, ir jānosaka skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma tvērumu un piemērošanu un paredz minimālas prasības, lai tā rezultātā personām, kuru dati tikuši pārsūtīti, būtu pietiekamas garantijas, kas ļautu viņu personas datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku. Tajā it īpaši ir jānorāda, kādos apstākļos un saskaņā ar kādiem nosacījumiem šādu datu apstrādi paredzošs pasākums var tikt veikts, tādējādi garantējot, ka šāda iejaukšanās notiek tikai stingri nepieciešamajā apmērā.[510]

Arī saskaņā ar ECT praksi prasība, ka ierobežojumam ir jābūt "paredzētam likumā", ir jāvērtē kopsakarā ar nepieciešamības un samērīguma prasību. ECTK 8. panta 2. punkts paredz: "Sabiedriskās institūcijas nedrīkst traucēt nevienam baudīt šīs tiesības [uz privātās dzīves neaizskaramību], izņemot gadījumos, kas ir paredzēti likumā un nepieciešami demokrātiskā sabiedrībā, lai aizsargātu valsts drošības, sabiedriskās kārtības vai valsts labklājības intereses, lai nepieļautu nekārtības vai noziegumus, lai aizsargātu veselību vai morāli, vai lai aizstāvētu citu tiesības un brīvības." ECT ir atzinusi, ka "tiesību kvalitāte" nozīmē, ka nacionālajiem tiesību aktiem jābūt ne tikai pieejamiem un paredzamiem attiecībā uz to piemērošanu, bet arī jānodrošina, lai slepeni novērošanas pasākumi tiktu piemēroti tikai tad, kad tas ir "nepieciešams demokrātiskā sabiedrībā", it īpaši jāparedz adekvātas un efektīvas aizsardzības garantijas pret ļaunprātīgu izmantošanu.[511] Valsts iestādēm ir zināma rīcības brīvība. Tomēr šī brīvība ir pakļauta Eiropas tiesību uzraudzībai, kas ietver gan tiesību aktus, gan lēmumus to piemērošanā. Tiesai jābūt pārliecinātai, ka pastāv pietiekamas un efektīvas garantijas pret ļaunprātīgu izmantošanu.[512] Šī jautājuma novērtējums ir atkarīgs no visiem lietā apskatāmajiem apstākļiem, piemēram, no iespējamo pasākumu rakstura,

509 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 168. punkts.

510 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 176. punkts.

511 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 236. punkts.

512 ECT 1978. gada 6. septembra spriedums lietā 5029/71, 50. punkts.

apjoma un ilguma, iemesliem, kas nepieciešami, lai tos piemērotu, no iestādēm, kas ir kompetentas tos atļaut, veikt un uzraudzīt, kā arī no tiesību aizsardzības līdzekļu veida. Ierobežojošo pasākumu noteikšanas un ieviešanas uzraudzības procedūrām jābūt tādām, lai saglabātu "iejaukšanos" tādu, kas ir "nepieciešama demokrātiskā sabiedrībā".[513]

Līdzīgi kā EST, arī ECT ir norādījusi, ka valsts slepeniem novērošanas pasākumiem ir jāatbilst "stingras nepieciešamības" kritērijam. Jebkādu iejaukšanos tiesībās uz privātumu atbilstoši ECTK 8. panta 2. punktam var attaisnot tikai tad, ja tā ir saskaņā ar likumu, tai ir viens vai vairāki likumīgi mērķi, kas noteikti minētajā normā, un tā ir nepieciešama demokrātiskā sabiedrībā, lai sasniegtu šādu mērķi. Tā kā šis noteikums paredz izņēmumu no tiesībām, kuras garantē ECTK, tas ir jāinterpretē šauri. Lietā "Klāss un citi pret Vāciju" ECT nosprieda, ka "pilsoņu slepenas novērošanas pilnvaras saskaņā ar ECTK ir pieļaujamas tikai tiktāl, ciktāl tas ir nepieciešams demokrātisku institūciju aizsardzībai"[514].

ECT lietā "Szabó un Vissy pret Ungāriju" arī atzīst, ka izteiciens "absolūti nepieciešams" no pirmā acu uzmetiena ir tests, kas atšķiras no tā, kas noteikts ECTK 8. panta 2. punkta redakcijā, tas ir, "nepieciešams demokrātiskā sabiedrībā".[515] Ņemot vērā attiecīgās iejaukšanās īpašo raksturu un modernāko novērošanas tehnoloģiju potenciālo aizskārumu pilsoņu privātumam, ECT uzskata, ka prasība "nepieciešams demokrātiskā sabiedrībā" ir jāinterpretē kā prasība pēc "stingras nepieciešamības" divos aspektos. Var uzskatīt, ka slepeni novērošanas pasākumi atbilst ECTK tikai tad, ja tas ir absolūti nepieciešams demokrātisku institūciju aizsardzībai, un turklāt, ja tas ir absolūti nepieciešams vitāli svarīgas informācijas iegūšanai individuālā operācijā. Jebkurš slepens novērošanas pasākums, kas neatbilst "stingras nepieciešamības" kritērijam, var būt pakļauts varas iestāžu ļaunprātīgai izmantošanai ar to rīcībā esošajām tehnoloģijām. Turklāt ECT vērš uzmanību, ka gan EST, gan ANO īpašais referents jautājumos par uzskatu un vārda brīvības tiesību veicināšanu un aizsardzību pieprasa, lai slepeni novērošanas pasākumi atbilstu stingras nepieciešamības kritērijam. Turklāt šajā kontekstā ECT īpaši uzsver iepriekšējas tiesas atļaujas nozīmi. Šī garantija ļauj ierobežot tiesībaizsardzības iestāžu rīcības brīvību, interpretējot plašu jēdzienu – "attiecīgās personas, kas identificētas [..] kā personu loks", lai pārbaudītu, vai katrā konkrētajā gadījumā personas saziņas pārtveršanai ir pietiekami iemesli. Tikai

513 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 232. punkts un tajā citētā judikatūra.

514 ECT 1978. gada 6. septembra spriedums lietā 5029/71, 42. un 54. punkts. Skat. arī ECT 2016. gada 12. janvāra spriedumu lietā 37138/14, 54. punkts.

515 ECT 2016. gada 12. janvāra spriedums lietā 37138/14, 72. punkts.

tādā veidā var apmierināt nepieciešamību pēc drošības pasākumiem, lai ārkārtas pasākumus izmantotu ierobežoti un tikai pienācīgi pamatotos gadījumos.[516]

Norāde, ka iejaukšanās "nepieciešama demokrātiskā sabiedrībā", ir jāinterpretē kā prasība, lai visi veiktie pasākumi būtu "absolūti nepieciešami" gan kā vispārējs apsvērums, lai aizsargātu demokrātiskas institūcijas, gan kā īpašs apsvērums, lai iegūtu būtisku informāciju konkrētajā gadījumā, lai novērstu draudus valsts vai sabiedrības drošībai vai noziedzīgu nodarījumu atklāšanai un nepieļaušanai.

ECT norādītie apsvērumi ir būtiski, izvērtējot jaunu mākslīgā intelekta novērošanas tehnoloģiju ieviešanu un izmantošanu. Pirms šādu tehnoloģiju ieviešanas ir jāizvērtē, vai tās ir vajadzīgas, jo "var palīdzēt" un "ir piemērotas", lai sasniegtu konkrēto mērķi, piemēram, lai garantētu valsts drošību, vai arī tās ir "stingri nepieciešamas" un nepastāv citu mazāk tiesības ierobežojošu veidu un līdzekļu, kā šo mērķi sasniegt. Tikai pēdējā gadījumā ierobežojumi var tikt atzīti par tiesiskiem.

5.3.3. Neatkarīgs uzraudzības mehānisms

Jau kopš 1978. gada lietas "Klāss un citi pret Vāciju" ECT daudzas reizes ir nospriedusi, ka ir būtiski, lai jebkāda iejaukšanās tiesībās uz privātumu un datu aizsardzību būtu pakļauta efektīvai, neatkarīgai un objektīvai uzraudzības sistēmai, ko nodrošina vai nu tiesnesis, vai cita neatkarīga struktūra. ECT ir norādījusi, ka slepenu novērošanas pasākumu pārbaude un uzraudzība var notikt trīs posmos: kad novērošana tiek noteikta pirmo reizi, kamēr tā tiek veikta un pēc tās izbeigšanas. Attiecībā uz pirmajiem diviem posmiem slepenas novērošanas būtība un loģika nosaka, ka tā jāveic bez personas ziņas. Līdz ar to, tā kā indivīdam obligāti tiks liegts pašam izmatot efektīvus tiesiskās aizsardzības līdzekļus vai tieši piedalīties jebkādās pārskatīšanas procedūrās, ir svarīgi, lai noteiktais process sniegtu pietiekamas un līdzvērtīgas garantijas, kas aizsargā viņa tiesības. Turklāt novērošanas procesā pēc iespējas precīzāk jāievēro demokrātiskas sabiedrības vērtības, lai netiktu pārsniegtas nepieciešamības robežas ECTK 8. panta 2. punkta izpratnē.

ECT ir norādījusi, ka slepenās novērošanas jomā, kur ļaunprātīga izmantošana ir potenciāli vienkārša un varētu radīt kaitīgas sekas demokrātiskai sabiedrībai kopumā, principā ir vēlams novērošanas kontroli uzticēt tiesnesim, ņemot

516 ECT 2016. gada 12. janvāra spriedums lietā 37138/14, 73. punkts.

vērā, ka tiesas kontrole nodrošina labākās neatkarības, objektivitātes un taisnīguma garantijas un pareizu procesa veikšanu.[517]

Kas attiecas uz trešo posmu, pēc novērošanas pabeigšanas jautājums par novērošanas pasākumu turpmāku paziņošanu ir nesaraujami saistīts ar tiesvedībā izmantojamo tiesiskās aizsardzības līdzekļu efektivitāti un līdz ar to ar efektīvu garantiju esamību pret novērošanas pilnvaru ļaunprātīgu izmantošanu. Attiecīgajai personai principā ir maz iespēju vērsties tiesā, izņemot, ja pastāv šādi apstākļi: ja persona ir informēta par pasākumu veikšanu bez viņa ziņas, un tādējādi tā ar atpakaļejošu spēku var apstrīdēt pasākumu likumību; vai arī – tiesā var vērsties jebkura persona, kurai ir aizdomas, ka tās saziņa tiek vai ir pārtverta, bet tiesas piekritība nedrīkstētu būt atkarīga no tā, vai šai personai ir paziņots, ka tās saziņa tikusi pārtverta.[518]

Tajā pašā laikā ECT 2018. gada spriedumā apvienotajās lietās "Big Brother Watch u. c. pret Apvienoto Karalisti" vērš uzmanību, ka objektīvu pierādījumu pieprasīšana par pamatotām aizdomām attiecībā uz personām, par kurām tiek meklēti dati, un sekojošais paziņojums novērošanas subjektam būtu pretrunā ar ECT atziņu, ka liela apjoma datu pārtveršanas režīma darbība principā ietilpst valsts rīcības brīvībā. Liela apjoma datu pārtveršana pēc definīcijas nav mērķtiecīga, un, pieprasot "pamatotas aizdomas", šādas shēmas darbība būtu neiespējama. Tāpat prasība par "turpmāku paziņošanu" paredz skaidri definētu novērošanas mērķu esamību, kas vienkārši nenotiek lielapjoma pārtveršanas režīmā. Turpretim tiesas atļauja pēc būtības nav nesaderīga ar masveida pārtveršanas efektīvu darbību.[519]

ECT lietā vērš uzmanību, ka tā jau iepriekš ir norādījusi – "vēlams novērošanas jurisdikciju uzticēt tiesnesim", jo novērošanas slepenā rakstura dēļ indivīds parasti nevarēs pats izmeklēt tiesiskās aizsardzības līdzekļus. Tajā pašā laikā ECT iepriekš to nav uzskatījusi "nepieciešamu prasību". ECT norāda, ka "negodīga, nolaidīga vai pārāk dedzīga ierēdņa nepareizas rīcības iespēju nekad nevar pilnībā izslēgt neatkarīgi no sistēmas". ECT atsaucas uz tās iepriekšējo judikatūru, kur var atrast daudzus piemērus gadījumiem, kad iepriekšēja tiesas atļauja nodrošināja tikai ierobežotu aizsardzību pret datu ļaunprātīgu izmantošanu vai to vispār nenodrošināja.[520] Piemēram, lietā "Roman Zakharov pret Krieviju" jebkurai saziņas pārtveršanai bija jāsaņem tiesas atļauja, un tiesnesim bija jāpamato

517 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 233. punkts; ECT 1978. gada 6. septembra spriedums lietā 5029/71, 55.–56. punkts.

518 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 234. punkts; ECT 1978. gada 6. septembra spriedums lietā 5029/71, 57. punkts.

519 ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13 .., 310., 315.–320. punkts.

520 Turpat, 319. punkts.

lēmums atļaut datu pārtveršanu. Tomēr, tā kā tiesas pārbaudes darbības joma bija ierobežota un policijai bija tehniski līdzekļi, lai apietu atļaujas piešķiršanas procedūru un pārtvertu jebkādu saziņu, iepriekš nesaņemot tiesas atļauju, ECT atzina, ka Krievijas likumi nespēj nodrošināt, ka "iejaukšanās" nepārkāpj kritērija "nepieciešams demokrātiskā sabiedrībā" robežas.[521] Lietā "Mustafa Sezgin Tanrıkulu pret Turciju" ECT konstatēja ECTK 8. panta pārkāpumu, kad krimināltiesa pusotru mēnesi bija piešķīrusi Nacionālajai izlūkošanas aģentūrai atļauju pārtvert visus vietējos un starptautiskos sakarus, lai identificētu personas, kas tika turētas aizdomās par terorismu.[522]

ECT lietā "Big Brother Watch u. c. pret Apvienoto Karalisti" secina, lai arī tā tiesas atļauju uzskata par svarīgu drošības līdzekli un varbūt pat par labo praksi, pati par sevi tā nevar būt ne vajadzīga, ne pietiekama, lai nodrošinātu ECTK 8. panta ievērošanu. Drīzāk ir jāņem vērā saziņas pārtveršanas sistēmas faktiskā darbība, tostarp varas izmantošanas pārbaudes un līdzsvars, kā arī faktiskas ļaunprātīgas izmantošanas pierādījumu esamība vai neesamība. Attiecīgi ECT izskatīja jebkādas iejaukšanās pamatojumu lietā, atsaucoties uz sešām obligātajām prasībām, kuras iepriekš izstrādātas tās judikatūrā par saziņas pārtveršanu kriminālizmeklēšanā un kuras būtu jānosaka tiesību aktā, lai izvairītos no varas ļaunprātīgas izmantošanas:

1) nodarījumu veids, kas var izraisīt noklausīšanās rīkojumu;
2) to cilvēku kategoriju definīcija, kuru saziņa var tikt pārtverta;
3) pārtveršanas ilguma ierobežojums;
4) prasības, kas jāievēro, pārbaudot, izmantojot un uzglabājot iegūtos datus;
5) piesardzības pasākumi, kas jāievēro, paziņojot datus citām pusēm;
6) apstākļi, kādos pārtvertos datus var dzēst vai iznīcināt.[523]

Lai gan ECT ņēma vērā arī citus attiecīgos faktorus, kurus tā identificēja lietā "Roman Zakharov pret Krieviju", proti, kārtību slepenu novērošanas pasākumu īstenošanas uzraudzībai, jebkuri paziņošanas mehānismi un valsts tiesību aktos paredzētie tiesiskās aizsardzības līdzekļi tomēr nekvalificēja šos pasākumus kā minimālās prasības.

Arī ES regulējums paredz neatkarīgas uzraudzības prasību. Hartas 8. panta 3. punkts nosaka, ka atbilstību tiesībām uz personas datu aizsardzību, kas paredzētas minētā panta 1. un 2. punktā, kontrolē neatkarīga iestāde.

Saistībā ar dalībvalstu tiesību aktiem EST ir identificējusi vairākus pasākumus, kas ir atbilstoši ES tiesību aktiem tikai tad, ja tos efektīvi pārskata tiesa vai administratīva iestāde, kuras lēmums ir saistošs.

521 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 232. punkts.

522 ECT 2017. gada 18. jūnija spriedums lietā 27473/06, 64. punkts.

523 ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13 .., 307., 320. punkts.

EST spriedumā apvienotajās lietās "Tele2 Sverige AB" un "Watson u. c.", atsaucoties uz ECT judikatūru, vērš uzmanību – tā kā vispārēja piekļuve visiem saglabātajiem datiem, kas nav atkarīga no jebkādas, kaut arī netiešas saiknes ar sasniedzamo mērķi, nevar tikt uzskatīta par tādu, kas aprobežojas ar absolūti nepieciešamo, attiecīgajam valsts tiesiskajam regulējumam ir jābalstās uz objektīviem kritērijiem, lai definētu apstākļus un nosacījumus, saskaņā ar kuriem kompetentajām valsts iestādēm piešķir piekļuvi abonentu vai reģistrēto lietotāju datiem. Šajā ziņā piekļuvi saistībā ar mērķi apkarot noziedzību var piešķirt vienīgi to personu datiem, kuras tiek turētas aizdomās par smaga nozieguma plānošanu, sagatavošanos tam vai tā izdarīšanu vai arī kuras vienā vai otrā veidā ir saistītas ar šādu noziegumu. Tomēr īpašos gadījumos, proti, kad vitāli svarīgas valsts drošības, aizsardzības vai sabiedrības drošības intereses apdraud teroristiskas darbības, piekļuvi var piešķirt arī citu personu datiem, ja pastāv objektīvi apstākļi, kas ļauj uzskatīt, ka šie dati konkrētajā gadījumā varētu sniegt efektīvu ieguldījumu šādu darbību apkarošanā.[524] Lai praksē nodrošinātu šo nosacījumu ievērošanu pilnībā, ir būtiski, ka kompetento valsts iestāžu piekļuve saglabātajiem datiem, izņemot atbilstoši pamatotus steidzamības gadījumus, principā ir pakļauta kontrolei un to veic tiesa vai neatkarīga administratīva iestāde, un šīs tiesas vai šīs iestādes lēmums tiek pieņemts pēc tam, kad šīs iestādes iesniegušas pamatotu pieteikumu, tostarp saistībā ar noziedzīga nodarījuma novēršanu, atklāšanu vai kriminālvajāšanas procedūrām.[525]

EST ir vērsusi uzmanību uz neatkarīgas tiesas nozīmi pār novērošanas programmu īstenošanu, kas paredz liela apjoma datu apstrādi, un arī gadījumos, kad tā neattiecas uz individuālu novērošanas pasākumu īstenošanu.[526]

Lietā "La Quadrature du Net u. c.", kurā EST noteica, ka izņēmuma gadījumā var paredzēt visaptverošus un nediferencētus datu saglabāšanas pasākumus, tā arī norādīja, ka, ņemot vērā no tiem izrietošās iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās smagumu, ir jānodrošina, lai šo pasākumu izmantošana patiešām attiektos tikai uz situācijām, kurās pastāv nopietns apdraudējums valsts drošībai. Šajā ziņā ir būtiski, lai lēmumu, ar kuru elektronisko komunikāciju pakalpojumu sniedzējiem tiek uzdots veikt šādu datu saglabāšanu, varētu efektīvi kontrolēt vai nu tiesa, vai arī neatkarīga administratīva iestāde, kuras

524 EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15 .., 118., 119. punkts.

525 Turpat, 120. punkts un tajā minētā judikatūra. Sk. arī EST 2009. gada 7. maija spriedumu lietā C-553/07 *Rijkeboer*, ECLI:EU:C:2009:293, 52. punkts, EST 2015. gada 6. oktobra spriedumu lietā C-362/14, 95. punkts.

526 Sk., piemēram, EST 2020. gada 16. jūlija spriedumu lietā C-311/18, 179., 183. punkts.

lēmumam ir saistoša iedarbība, lai pārbaudītu, vai pastāv šāda situācija, kā arī – vai ir ievēroti paredzētie nosacījumi un garantijas.[527]

Tāpat EST minētajā lietā norādīja, ka ir būtiski, lai pasākuma, ar kuru atļauj reāllaikā vākt informāciju par datu plūsmu un atrašanās vietas datus, īstenošana būtu pakļauta iepriekšējai pārbaudei, ko veic tiesa vai neatkarīga administratīva iestāde, kuras lēmumam ir saistoša iedarbība, un ka šai tiesai vai šai iestādei turklāt ir jāpārliecinās, ka šāda vākšana reāllaikā tiek atļauta vienīgi absolūti nepieciešamā robežās. Pienācīgi pamatotos neatliekamības gadījumos pārbaude jāveic īsā laikā.[528]

Neatkarīgas uzraudzības iestādes kontrolei ir būtiska nozīme, lai pārbaudītu, vai pastāv situācija, kas pamato pasākumu piemērošanu, un vai ir ievēroti nosacījumi un aizsardzības garantijas. Neatkarīgam uzraudzības mehānismam ir jābūt izveidotam, arī lai kontrolētu mākslīgā intelekta novērošanas pasākumus. Līdzās neatkarīgam uzraudzības mehānismam ir jābūt pieejamiem arī efektīviem tiesību aizsardzības līdzekļiem.

5.3.4. Efektīvi tiesību aizsardzības līdzekļi

Pēdējā būtiskā garantija ir saistīta ar tiesībām uz efektīviem tiesiskās aizsardzības līdzekļiem, lai aizsargātu personas tiesības, ja viņa uzskata, ka tās netiek ievērotas. Minētās tiesības ir noteiktas Hartas 47. pantā, kura pirmā daļa paredz, ka ikvienai personai, kuras tiesības un brīvības, kas garantētas ES tiesībās, tikušas pārkāptas, ir tiesības uz efektīvu tiesību aizsardzību tiesā. Hartas 47. panta otrā daļa paredz ikvienas personas tiesības uz taisnīgu, atklātu un laikus veiktu lietas izskatīšanu neatkarīgā un objektīvā, tiesību aktos noteiktā tiesā. EST "Schrems I" lietā vērš uzmanību, ka tiesiskai valstij ir raksturīga pārbaude tiesā, un tās mērķis ir nodrošināt ES tiesību normu ievērošanu. Tiesiskajā regulējumā, kurā indivīdiem nav paredzētas nekādas iespējas izmantot tiesību aizsardzības līdzekļus, lai piekļūtu personas datiem, kas uz tiem attiecas, vai panāktu šādu datu labošanu vai dzēšanu, nav ņemta vērā Hartas 47. pantā paredzēto pamattiesību uz efektīvu aizsardzību tiesā būtība.[529]

Efektīvu tiesību aizsardzība ir nesaraujami saistīta ar tiesībām uz informāciju. Lai personas varētu aizstāvēt savas tiesības, viņām ir jāpaziņo par novērošanas pasākumu piemērošanu pēc novērošanas pasākuma pabeigšanas. EST lietā "Tele 2 Sverige AB" norāda – ir būtiski, ka kompetentās valsts iestādes, kurām ir piešķirta piekļuve saglabātajiem datiem, par to informē attiecīgās personas

527 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 139. punkts.

528 Turpat, 189. punkts.

529 EST 2015. gada 6. oktobra spriedums lietā C-362/14, 95. punkts.

atbilstoši piemērojamajām valsts procesuālajām normām no brīža, kad šī saziņa vairs nevar traucēt šo iestāžu veiktajai izmeklēšanai. Proti, šī informēšana faktiski ir nepieciešama, lai ļautu šīm personām to tiesību pārkāpuma gadījumā īstenot tiesības uz tiesisko aizsardzību.[530]

Lietā "La Quadrature du Net u. c." EST norāda, ka ir būtiski, lai kompetentās valsts iestādes, kuras veic informācijas par datu plūsmu un atrašanās vietas datu vākšanu reāllaikā, par to informētu datu subjektus atbilstoši piemērojamajām valsts procesuālajām normām tiktāl un no brīža, kad šī informēšana vairs nevar traucēt šo iestāžu uzdevumu izpildi. Šī informēšana faktiski ir nepieciešama, lai ļautu šīm personām īstenot to tiesības, kas izriet no Hartas 7. un 8. panta, lūgt piekļuvi saviem personas datiem, kas ir šo pasākumu priekšmets, un vajadzības gadījumā panāktu to labošanu vai dzēšanu, kā arī saskaņā ar Hartas 47. panta pirmo daļu izmantotu tiesības uz efektīvu tiesību aizsardzību tiesā.[531] Attiecībā uz informēšanu, kas tiek prasīta informācijas par datu plūsmu un atrašanās vietas datu automatizētas analīzes kontekstā, jānorāda, ka kompetentajai valsts iestādei ir jāpublicē vispārēja rakstura informācija par šo analīzi, taču tai nav pienākuma individuāli informēt datu subjektus. Savukārt gadījumā, ja dati atbilst pasākumā, ar ko atļauta automatizētā analīze, precizētajiem parametriem un ja kompetentā valsts iestāde identificē datu subjektu, lai padziļināti analizētu datus, kas uz viņu attiecas, ir nepieciešams šo personu informēt individuāli. Tomēr šāda informācija ir jāsniedz tikai un vienīgi tādā apmērā un no tā brīža, kad tā nevar apdraudēt minētajai iestādei uzticēto uzdevumu izpildi.[532]

Tomēr EST lietā "La Quadrature du Net u. c." nesniedz norādes, vai izņēmuma gadījumā, kad pastāv nopietni draudi valsts drošībai un preventīvi ir paredzēta informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana, būtu jāinformē par to personas. EST vienīgi vispārīgi norāda, ka attiecīgo datu saglabāšanai jānotiek atbilstoši tai paredzētajiem materiāltiesiskajiem un procesuālajiem nosacījumiem un ka datu subjektiem ir efektīvas garantijas pret ļaunprātīgas izmantošanas risku.[533]

Kā uzsvērusi arī ECT, lai persona varētu efektīvi izmantot tiesību aizsardzības līdzekļus, tai ir jābūt informētai par pasākumiem, kas tiek veikti pret viņu. Veicot slepenu novērošanu, pēc tās beigām persona ir jāinformē par pret viņu veiktajiem pasākumiem. Personai principā ir maz iespēju vērsties tiesā, ja vien viņa nav informēta par pasākumu veikšanu bez viņa ziņas, un tad šī persona ar atpakaļejošu spēku var apstrīdēt to likumību, vai arī persona var vērsties tiesā,

530 EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15, 121. punkts.

531 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 190. punkts.

532 Turpat, 191. punkts.

533 Turpat, 168. punkts.

ja tai ir aizdomas, ka viņa saziņa tiek vai ir pārtverta.[534] Tajā pašā laikā lietā "Big Brother Watch u. c. pret Apvienoto Karalisti" ECT atzīst, ka prasība pēc "turpmākas paziņošanas" paredz skaidri definētu novērošanas mērķu esamību, kas vienkārši nenotiek lielapjoma jeb masveida datu pārtveršanas režīmā.[535]

Ikvienas personas tiesības efektīvi aizstāvēt savas tiesības ir būtiskas, ja pret personu tiek piemēroti masveida novērošanas pasākumi, it īpaši, ja tie šo personu skar tieši un ietekmē lēmumu pieņemšanu pret personu, piemēram, aizturēšanu. Vienlaicīgi, lai tiktu nodrošinātas efektīvas garantijas pret uzraudzības pilnvaru ļaunprātīgu izmantošanu, turklāt ņemot vērā ierobežotās iespējas katrai atsevišķai personai aizstāvēt savas tiesības, būtiska nozīme ir nevalstisko un tiesību aizsardzības organizāciju darbībai. Kā jau iepriekš norādīts, ECT masveida novērošanas lietās pieņem arī kolektīvās sūdzības. Piemēram, ECT "Big Brother Watch u. c. pret Apvienoto Karalisti" lietā pieteicēji bija vairāk nekā desmit nevalstiskās un tiesību aizstāvības organizācijas.[536] Pilsoniskā līdzdalība ir būtiska garantija, lai uzraudzītu valsts piemēroto pasākumu likumību un novērstu varas ļaunprātīgu izmantošanu.

Nodaļā apskatītā ECT un EST tiesu prakse apstiprina, ka masveida novērošanas pasākumi rada būtisku iejaukšanos privātumā un datu aizsardzībā. Kā visbūtiskākais nosacījums, piemērojot masveida novērošanas pasākumus, ir norādīts pienākums izvērtēt, vai piemērotie pasākumi ir "stingri" jeb "absolūti" nepieciešami konkrētā mērķa sasniegšanai un vai tie ir samērīgi jeb proporcionāli ar šo mērķi. Visās lietās ir uzsvērta nepieciešamība tiesību aktos noteikt atbilstošas procesuālās garantijas, it īpaši tiesas vai neatkarīgas iestādes kontroli un pienākumu informēt personas par šādu pasākumu piemērošanu.

Šos nosacījumus ir būtiski ievērot arī pirms jaunu novērošanas tehnoloģiju ieviešanas. Vairāki gadījumi attiecībā uz sejas atpazīšanas tehnoloģiju piemērošanu liecina, ka praksē bieži vien tās tiek ieviestas, neizvērtējot, vai tas ir "stingri" jeb "absolūti" nepieciešams un vai tas ir samērīgi, kā arī tās tiek izmantotas slepeni, neinformējot personas un sabiedrību.[537] Lai izvērtētu novērošanas pasākumu nepieciešamību, ir jāizvērtē šo pasākumu piemērotība un efektivitāte, lai sasniegtu mērķi, un jāizvērtē, vai ir izvēlēts vismazāk aizskarošs līdzeklis. Tajā pašā laikā to izdarīt ir ļoti problemātiski, jo trūkst empīrisko pierādījumu par

534 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 234. punkts; ECT 1978. gada 6. septembra spriedums lietā 5029/71, 57. punkts; ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13 .., 310. punkts.

535 ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13 .., 317. punkts.

536 Sk. ECT 2018. gada 13. septembra spriedumu apvienotajās lietās 58170/13 .., Appendix. List of Applicants.

537 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

šādu pasākumu efektivitāti.[538] Nav pieļaujams, ka masveida novērošanas pasākumi, kas būtiski ierobežo personu pamattiesības, to skaitā tādi, kas izmanto jaunās novērošanas tehnoloģijas, tiek ieviesti un piemēroti, neizvērtējot to proporcionalitāti un nepieciešamību, nenodrošinot atbilstošas procesuālas garantijas un it īpaši – neinformējot personas. Šāda prakse neatbilst tiesiskas valsts principa prasībām un var apdraudēt demokrātiju.

Plašā EST un ECT prakse sniedz būtiskas vadlīnijas, kā izvērtēt, vai plānotie vai esošie novērošanas pasākumi ir atbilstoši tiesību uz privātumu un datu aizsardzību ierobežošanas nosacījumiem. Tajā pašā laikā ir svarīgi, lai Hartas 8. pantā noteiktās tiesības uz personas datu aizsardzību garantētu plašu aizsardzību, kas ietver ne tikai šī panta 2. un 3. punktā tieši paredzētās garantijas, bet arī citus būtiskus datu aizsardzības principus un garantijas, kas noteiktas galvenajos ES datu aizsardzības tiesību aktos.[539] Hartas 8. panta 2. punkts nosaka personas datu apstrādes nosacījumus, proti, šādi dati ir jāapstrādā godprātīgi, noteiktiem mērķiem un ar likumīgu pamatojumu, kas paredzēts tiesību aktos. Harta arī paredz, ka ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un ir tiesības ieviest labojumus šajos datos. Hartas 8. panta 3. punkts savukārt paredz, ka atbilstību šiem noteikumiem ir jākontrolē neatkarīgai iestādei. EST bieži ir atsaukusies uz šajās normās noteiktajām garantijām. Tajā pašā laikā masveida novērošanas pasākumiem ir jāatbilst dažādiem principiem un prasībām, kas paredzētas VDAR un citos datu aizsardzības tiesību aktos. Šīs prasības aplūkotas nākamajā grāmatas nodaļā.

538 Sk. Tzanou (2019), *The Fundamental Right to Data Protection*, p. 253.

539 Ibid., p. 255.

6. DAĻA

Datu aizsardzības pamatprasības mākslīgā intelekta novērošanas tehnoloģijām

Datu aizsardzības tiesības ir galvenais regulējums, kas jau šobrīd ir piemērojams attiecībā uz mākslīgo intelekta sistēmu izstrādi, ieviešanu un izmantošanu, tiklīdz tās skar personas datu apstrādi. Datu aizsardzības regulējums palīdz novērst radīto apdraudējumu ne tikai tiesībām uz privātumu un datu aizsardzību, bet arī citām pamattiesībām, piemēram, diskriminācijas aizlieguma principam. Kā tika atklāts iepriekšējā nodaļā, tas lielā mērā ietekmē un uz to ir balstīta mākslīgā intelekta regulējuma turpmākā attīstība. Jautājums ir, ciktāl Eiropā pastāvošais datu aizsardzības regulējums var palīdzēt novērst mākslīgā intelekta novērošanas sistēmu radītos riskus cilvēktiesībām un nodrošināt to atbildīgu izstrādi, ieviešanu un izmantošanu. Vai datu aizsardzības regulējums ir pietiekams, vai arī gluži pretēji – būtu nepieciešams speciāls regulējums attiecībā uz noteiktiem mākslīgā intelekta izmantošanas veidiem, nosakot jaunas prasības un ierobežojumus?

Datu aizsardzības regulējums izvirza daudzas prasības mākslīgā intelekta un cita veida novērošanas tehnoloģijām un paredz speciālus noteikumus attiecībā uz biometrisko datu apstrādi. Šajā nodaļā izvērtētas būtiskākās datu aizsardzības prasības, kas ir piemērojamas mākslīgā intelekta novērošanas pasākumiem, un vērsta uzmanība uz galvenajiem problēmjautājumiem, īpašu uzmanību veltot sejas atpazīšanas tehnoloģijām. Nodaļā aplūkoti un salīdzināti noteikumi, kas ietverti VDAR, kura paredz vispārējās prasības, un Policijas direktīvā, kura ir piemērojama attiecībā uz tiesībaizsardzības iestādēm, kā arī Konvencijā 108+ ietvertās normas, kuras vērš uzmanību uz kopīgajām un atšķirīgajām garantijām. Nodaļas nobeigumā atsevišķi aplūkoti datu aizsardzības standarti, kas ietverti starptautisko organizāciju izdotajās rekomendācijās kontaktu izsekošanas lietotnēm, un būtiskie izaicinājumi to piemērošanā praksē, vēršot uzmanību uz nepieciešamību minētos standartus attiecināt arī uz mākslīgā intelekta novērošanas tehnoloģijām.

6.1. Personas datu apstrāde un biometriskā novērošana

Datu aizsardzības tiesību centrālais elements ir personas datu jēdziens, kas nosaka datu aizsardzības tiesību aktu materiālo piemērošanu.

VDAR un Policijas direktīvā ir sniegta vienāda personas datu definīcija: “Personas dati ir jebkura informācija, kas attiecas uz identificētu vai identificējamu

fizisku personu ("datu subjektu"); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, it īpaši, atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem." (VDAR 4. panta 1. punkts, Policijas direktīvas 3. panta 1. punkts). Konvencija 108+ personas datus definē īsāk, kā "jebkuru informāciju, kas attiecas uz identificētu vai identificējamu personu (datu subjektu)" (2. panta a) punkts).

Par personas datiem netiek uzskatīta informācija, kas, lai gan attiecas uz cilvēkiem, neattiecas uz konkrētu personu. Lai šādu informāciju atzītu par personas datiem, personai ir jābūt "identificētai vai identificējamai". Persona ir identificējama, ja tā vēl nav identificēta, bet to ir iespējams identificēt. Lai noteiktu, vai fizisku personu ir iespējams identificēt, ir jāņem vērā visi līdzekļi, ko varētu izmantot, piemēram, atsevišķa izdalīšana, lai tieši vai netieši identificētu fizisku personu (VDAR 26. apsvērums).

Gan VDAR, gan Policijas direktīva atsevišķi izdala īpašu kategoriju personas datus, kuriem paredzēta augstāka aizsardzība. Abi tiesību akti skaidro, ka tie ir tādi personas dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, ģenētiskie dati, biometriskie dati, kas ļauj veikt fiziskas personas unikālu identifikāciju, veselības dati un dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju (VDAR 9. panta 1. punkts, Policijas direktīvas 10. pants). Konvencijas 108+ 6. pants paredz, ka īpašu kategoriju datu apstrāde ietver: ģenētisko datu apstrādi; personas datus, kas attiecas uz noziedzīgiem nodarījumiem, kriminālprocesiem, notiesājošiem spriedumiem un saistītiem drošības pasākumiem; biometriskos datus, kas unikāli identificē personu; personas datus attiecībā uz informāciju, ko tie atklāj, saistībā ar rasi vai etnisko izcelsmi, politiskajiem uzskatiem, dalību arodbiedrībās, reliģisko vai citu pārliecību, veselību vai seksuālo dzīvi.

Gan VDAR, gan Policijas direktīva sniedz arī identisku biometrisko datu definīciju: "Biometriskie dati ir personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprina minētās fiziskās personas unikālu identifikāciju, piemēram, sejas attēli vai daktiloskopijas dati." (VDAR 4. panta 14. punkts, Policijas direktīvas 3. panta 13. punkts.)

ES datu aizsardzības regulējumā biometrisko datu definīcija ir formulēta plaši, lai tā aptvertu fiziskās, fizioloģiskās vai uzvedības pazīmes. Par biometriskiem datiem ir atzītas dažādas informācijas kategorijas: tās var būt "fiziskās / fizioloģiskās īpašības" (piemēram, sejas vaibsti, pirkstu nospiedumi), bioķīmiskas pazīmes (DNS), kā arī motorika vai dažādi uzvedības raksturlielumi (ieradumi, personības

iezīmes, atkarības, gaita, taustiņu nospiešanas veids utt.).[540] Digitālie sejas attēli pieder pie pirmās kategorijas, vienlaicīgi, ja tiek izmantotas, piemēram, emocionālās uztveršanas sistēmas, tie var atklāt arī dažādas personības iezīmes.

Cilvēka sejas attēls ir uzskatāms par biometriskajiem datiem. Tas ir vairāk vai mazāk unikāls, kā arī tas maz mainās. To parasti nevar noslēpt, lai gan Covid-19 pandēmijas laikā sejas bieži aizsedza maskas. Sejas attēlu ir arī viegli iegūt, jo atšķirībā no DNS vai pirkstu nospiedumu iegūšanas procesa personai parasti ir grūti izvairīties no tās publiskas novērošanas.[541] Tajā pašā laikā sejas attēlu apstrādes konteksts ir būtisks, lai noteiktu datu sensitīvo raksturu, jo ne visa attēlu apstrāde ietver īpašu kategoriju personas datu apstrādi. Uz attēliem biometrisko datu definīcija attieksies tikai tad, ja tos apstrādā, izmantojot īpašu tehnisku līdzekli, kas ļauj unikāli identificēt vai autentificēt personu.[542] VDAR skaidro, ka fotogrāfiju apstrāde nebūtu vienmēr jāuzskata par īpašu kategoriju personas datu apstrādi, jo uz tām biometrisko datu definīcija attiecas tikai tad, kad tās apstrādās ar konkrētiem tehniskiem līdzekļiem, kas ļauj veikt fiziskas personas unikālu identifikāciju vai autentifikāciju (51. apsvērums).

Eiropas Datu aizsardzības kolēģija ir norādījusi, ka personas videomateriālu nevar uzskatīt par biometriskiem datiem saskaņā ar VDAR 9. pantu, ja tas nav īpaši tehniski apstrādāts, lai veicinātu personas identificēšanu. Lai to varētu uzskatīt par īpašu kategoriju personas datu apstrādi (9. pants), biometriskie dati ir jāapstrādā "fiziskas personas unikālas identificēšanas nolūkā". Ievērojot VDAR 4. panta 14. punktu un 9. pantu, jāņem vērā trīs kritēriji:

1) datu veids – dati par fiziskas personas fiziskām, fizioloģiskām vai uzvedības īpašībām;
2) apstrādes līdzekļi un veids – dati, kas iegūti "īpašā tehniskā apstrādē";
3) apstrādes mērķis – dati jāizmanto, lai unikāli identificētu fizisku personu.[543]

Biometriskie dati, kā tie ir definēti VDAR 4. panta 14. punktā un Policijas direktīvas 3. panta 13. punktā, ir personas datu apakškategorija, līdz ar to tiem ir jāatbilst šajos pantos minētajiem kritērijiem. Tas, cik lielā mērā biometriskās shēmas var uzskatīt par personas datiem, ir ilgstošu diskusiju temats.

Biometrisko sistēmu mērķis parasti ir personas identificēšana (personas identifikācija salīdzinājumā ar citu personu) vai personas autentifikācija, kas

540 Article 29 Data Protection Working Party. (2012). Opinion 3/2012 on developments in biometric technologies. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

541 FRA (2019), Facial recognition technology.

542 Council of Europe (2021), .. Convention 108.

543 EDPB. (2020). Guidelines 3/2019 on processing of personal data through video devices. Version 2.0. Adopted on 29 January 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

tiek saukta arī par verifikāciju (noteikšana, vai persona ir tā, par ko tā izliekas).[544] Abus jēdzienus ir skaidrojusi 29. panta darba grupa, kas norāda, ka "personas identificēšana, izmantojot biometrisko sistēmu, parasti ir process, kurā tiek salīdzināti indivīda biometriskie dati (kas iegūti identifikācijas brīdī) ar vairākām datubāzē glabātām biometriskām veidnēm (t. i., salīdzināšanas process "viens pret daudziem")", savukārt "personas verifikācija, izmantojot biometrisko sistēmu, parasti ir process, kurā salīdzina indivīda biometriskos datus (kas iegūti verifikācijas laikā) ar vienu biometrisko veidni, kas glabājas ierīcē (t. i., viens pret vienu salīdzināšanas process)".[545]

Biometrisko datu definīcija, liekas, aptver abus veidus, paredzot, ka tie "ļauj veikt vai apstiprina personas unikālu identifikāciju" (VDAR 4. panta 14. punkts; Policijas direktīvas 3. panta 13. punkts). Arī VDAR 51. pantā ir norādīts "ļauj veikt fiziskas personas unikālu identifikāciju". Tomēr šie dažādie mērķi netiek atkārtoti VDAR 9. panta 1. punktā un Policijas direktīvas 10. pantā, kas attiecībā uz personas datiem ir ierobežoti ar gadījumiem, kad dati tiek apstrādāti, lai veiktu fiziskas personas unikālu identifikāciju. Proti, VDAR 9. panta 1. punkts un Policijas direktīvas 10. pants ir attiecināms tikai uz biometriskajiem datiem, kas tiek izmantoti personas unikālai identifikācijai, bet ne autentifikācijai.[546]

FRA sejas atpazīšanas izmantošanu iedala trīs veidos: verifikācijai, identifikācijai un kategorizācijai.[547] Verifikācijas procedūru izmanto, piemēram, automatizētai robežkontrolei lidostu pārbaudēs. Persona ieskenē savu pases attēlu, un uz vietas tiek uzņemts attēls. Sejas atpazīšanas tehnoloģija salīdzina abus sejas attēlus, un, ja varbūtība, ka abi attēli parāda vienu un to pašu personu, pārsniedz noteiktu varbūtības slieksni, tiek apstiprināta identitāte. Pārbaude neprasa, lai biometriskās pazīmes tiktu glabātas centrālajā datubāzē. Tos var uzglabāt, piemēram, personas identitāti apliecinošā vai ceļošanas dokumentā.

Tiek uzskatīts, ka biometrisko datu izmantošana identifikācijai rada daudz lielāku apdraudējumu (tai skaitā no datu aizsardzības viedokļa), nekā to izmantošana autentifikācijai jeb verifikācijai. Sejas atpazīšanas tehnoloģijas tiek izmantotas personas identifikācijai, ja personas sejas attēls tiek salīdzināts ar daudziem citiem attēliem, kas glabājas datubāzē, lai uzzinātu, vai šī persona ir iekļauta konkrētajā datubāzē. Katram salīdzinājumam tiek dots konkrēts punktu skaits, norādot varbūtību, ka divi attēli attiecas uz vienu un to pašu personu. Dažreiz attēlus pārbauda, salīdzinot ar datubāzēm, kur ir zināms, ka persona, kuras attēls

544 Kuner, C., Bygrave, L. A., Docksey, C. (eds.). (2019). *The EU General Data Protection Regulation* (*GDPR*): *A Commentary*. Oxford, United Kingdom: Oxford University Press, p. 213.

545 Article 29 Data Protection Working Party (2012), Opinion 3/2012 ..

546 Kuner, Bygrave, Docksey (2019), *The EU General Data Protection Regulation* .., p. 214.

547 FRA (2019), Facial recognition technology.

tiek salīdzināts, atrodas datubāzē (slēgta datu kopas identifikācija), un dažreiz, – ja tas nav zināms (atvērta datus kopas identifikācija). Pēdējā darbība ir piemērota, ja personas tiek pārbaudītas pēc novērošanas sarakstiem. Sejas atpazīšanas tehnoloģijas izmantošanu identifikācijai dažkārt sauc par automatizētu sejas atpazīšanu.

Identifikāciju var veikt, izmantojot sejas attēlus, kas iegūti no videokamerām. Sejas attēli arī videomateriālos tiek iegūti un pēc tam salīdzināti ar sejas attēliem datubāzē, lai identificētu, vai videomateriālā redzamā persona ir atrodama attēlu datubāzē (meklējamo personu sarakstā). Ar videokamerām iegūto sejas attēlu kvalitāti nevar kontrolēt: gaisma, attālums un atrašanās vieta ierobežo videomateriālos uzņemtās personas sejas vaibstus. Tāpēc sejas atpazīšanas tehnoloģiju izmantošana, visticamāk, rada nepatiesas atbilstības salīdzinājumā ar sejas attēliem, kas uzņemti kontrolētā vidē, piemēram, robežas šķērsošanas vietā vai policijas iecirknī.

Sejas atpazīšanas tehnoloģijas tiek izmantota arī kategorizācijai.[548] Sejas attēlu var analizēt, kā arī var veikt tā saucamo emociju, uzvedības jeb afektīvo analīzi. To var izmantot arī indivīdu profilēšanai, kas ietver indivīdu kategorizāciju, pamatojoties uz viņu personīgajām īpašībām.[549] Pēc sejas attēliem parasti nosakāmās īpašības ir dzimums, vecums un etniskā izcelsme. Sejas atpazīšanas tehnoloģijas tiek izmantotas, lai atpazītu cilvēku emocijas, piemēram, dusmas, bailes vai laimes sajūtu, un lai noteiktu, vai cilvēki melo vai saka patiesību. Ir bijuši eksperimenti, izmantojot sejas attēlu, noteikt personas seksuālo orientāciju. Kategorizācijas gadījumā šīs tehnoloģijas netiek izmantotas indivīdu identifikācijai, bet gan indivīda raksturošanai, bet tas ne vienmēr ļauj personu identificēt. Tomēr, ja no sejas tiek secināti vairāki raksturlielumi un tie, iespējams, ir saistīti ar citiem datiem (piemēram, atrašanās vietas datiem), tas faktiski varētu ļaut identificēt personu.[550]

Profesors Dž. Sartors vērš uzmanību, ka mākslīgais intelekts izvirza jautājumus, kas saistīti ar personas datu būtību, it sevišķi attiecībā uz iespēju secināt jaunus personas datus no esošajiem datiem, kā arī iespēju atkal savienot datu subjektus ar viņu identificētajiem datiem. Šajā saistībā personas datu jēdziens, kas noteikts ES datu aizsardzības tiesību aktos, nesniedz skaidras atbildes. Zinātnieks

548 MI akta priekšlikums definē "biometriskās kategorizācijas sistēmu" kā mākslīgā intelekta sistēmu, kuras mērķis ir noteikt fizisku personu piederību noteiktām kategorijām, piemēram, tādām kā dzimums, vecums, matu krāsa, acu krāsa, tetovējumi, etniskā izcelsme vai seksuālā vai politiskā orientācija, pamatojoties uz viņu biometriskajiem datiem (1. panta 35. punkts); Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

549 Sk. FRA. (2018). Preventing unlawful profiling today and in the future: a guide. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

550 FRA (2019), Facial recognition technology.

uzskata, ka par personas datiem ir jāatzīst arī tā sauktie izsecināmie personas dati. Viņš norāda, ka mākslīgā intelekta algoritmi var izsecināt jaunu informāciju par datu subjektiem, viņu personas datiem.

No datu aizsardzības viedokļa galvenais jautājums ir, vai secinātā informācija būtu jāuzskata par jauniem personas datiem un vai tā ir nodalāma no datiem, no kuriem tā ir izsecināta. Pieņemsim, ka, piemēram, indivīda seksuālā orientācija tiek izsecināta no viņa sejas vai sejas īpašībām, vai no šīs personas aktivitātēm tiešsaistē. Vai izsecinātais seksuālās orientācijas vai personības veids būtu jauns personas datu elements? Pat tad, ja secinājums ir tikai varbūtīgs? Ja izsecinātā informācija tiek uzskatīta par jauniem personas datiem, tad attiecībā uz šādiem automatizētiem secinājumiem rastos pienākums ievērot visas prasības, kuras saskaņā ar datu aizsardzības noteikumiem ir noteiktas personas datu apstrādei: tiesiskā pamata nepieciešamību, nosacījumus sensitīvu datu apstrādei, datu subjekta tiesības utt. Iespējamā pieeja varētu būt to gadījumu nošķiršana, kuros personas datu izsecināšana tiek veikta, neveicot citas darbības, t. i., izsecinātie personas dati ir tikai aprēķina rezultāts, no kuriem neizriet tālākas darbības, atšķirībā no tiem gadījumiem, kad secināmos datus izmanto, lai veiktu novērtējumu un pieņemtu lēmumus. Pēdējā gadījumā dati noteikti būtu jāuzskata par jaunievāktiem personas datiem. [551]

Mākslīgā intelekta sistēmas palielina acīmredzami anonīmu datu identificējamību, jo tie ļauj neidentificētus datus, ieskaitot datus, kas ir anonimizēti vai pseidonimizēti[552], saistīt ar attiecīgajām personām. VDAR 26. apsvērumā un Policijas direktīvas 21. apsvērumā ir norādīts, ka "datu aizsardzības principi nebūtu jāpiemēro anonīmai informācijai, proti, informācijai, kura neattiecas uz identificētu vai identificējamu fizisku personu, vai personas datiem, ko sniedz anonīmi tādā veidā, ka datu subjekts nav vai vairs nav identificējams". Dž. Sartors norāda, ka būtu ieteicams precizēt, iespējams, nesaistošā tiesību aktā vai atzinumā, ka atkārtota identifikācija ir personas datu apstrāde un to patiešām var pielīdzināt jaunu personas datu vākšanai. Tāpēc uz atkārtotu identifikāciju pilnībā attiecas visas VDAR prasības, tostarp pienākums informēt datu subjektu un nepieciešamība pēc tiesiskā pamata.[553]

551 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

552 Pseidonimizācija ir personas datu apstrāde, ko veic tādā veidā, lai personas datus vairs nav iespējams saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka personas dati netiek saistīti ar identificētu vai identificējamu fizisku personu (VDAR 4. panta 5. punkts). VDAR 28. apsvērums paredz, ka personas dati, kuri ir pseidonimizēti un kurus, izmantojot papildu informāciju, varētu attiecināt uz fizisku personu, ir uzskatāmi par informāciju par identificējamu fizisku personu.

553 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

Īpašu kategoriju personas datu apstrāde, to skaitā biometrisko datu apstrāde, var radīt nopietnu risku pamattiesībām un brīvībām, tāpēc tiem ir noteikta īpaša aizsardzība (Policijas direktīvas 37. apsvērums, VDAR 51. apsvērums). VDAR aizliedz īpašu kategoriju datu apstrādi, ja vien nepastāv kāds no VDAR konkrēti paredzētiem pamatojumiem. Policijas direktīva un Konvencija 108+ atļauj šādu datu apstrādi, ja tiek ievēroti stingri nosacījumi, kas aplūkoti nākamajā apakšnodaļā.

6.2. Personas datu apstrādes pamatprincipi

Personas datu apstrādes principi ir pamatā un jāpiemēro, interpretējot pārējās datu aizsardzības prasības. Pamatprincipi, kas tika ietverti, piemēram, 1981. gada Konvencijā 108, nav būtiski mainījušies, ja tos salīdzina ar citām datu aizsardzības prasībām, kas ir attīstījušās vairākus gadsimtus. Tie ir izturējuši laika pārbaudi un var tikt piemēroti dažādos tehniskos, ekonomiskos un sociālos kontekstos.[554] Datu aizsardzības principi ir piemērojami arī mākslīgā intelekta tehnoloģijām. VDAR 5. pants nosaka šādus personas datu apstrādes principus: likumīgums, godprātība un pārredzamība, nolūka ierobežojums, datu minimizēšana, precizitāte, glabāšanas ierobežojums, integritāte un konfidencialitāte, pārskatatbildība. Policijas direktīvas 4. pants paredz gandrīz visus tos pašus principus, izņemot pārredzamības un pārskatatbildības principu. Daži no principiem ir tālāk attīstīti turpmākajos pantos, piemēram, likumības princips, kas noteikts VDAR 5. panta 1. punkta a) apakšpunktā un Policijas direktīvas 4. panta 1. punkta a) apakšpunktā, ir tālāk skaidrots VDAR 6. pantā un Policijas direktīvas 8. pantā.

6.2.1. Likumīgums, tiesiskais pamats un nolūka ierobežojuma princips

VDAR kā pirmos principus paredz, ka personas dati tiek apstrādāti likumīgi, godprātīgi un datu subjektiem pārredzamā veidā (5. panta 1. punkta a) apakšpunkts). Policijas direktīva nosaka, ka personas dati tiek apstrādāti likumīgi un godprātīgi (4. panta 1. punkta a) apakšpunkts). Arī Konvencijā 108+ ir noteikts, ka personas datus apstrādā likumīgi (5. panta 3. punkts).

No likumīguma principa izriet vispārējs nosacījums, ka personas dati jāapstrādā, ievērojot tiesību aktos noteiktās prasības. Saskaņā ar VDAR un Policijas direktīvu likumīguma princips paredz, ka datu apstrādei, lai tā būtu likumīga, ir jābūt tiesiskam pamatam. VDAR 6. panta 1. punkts paredz, ka personas datu

554 Kuner, Bygrave, Docksey (2019), *The EU General Data Protection Regulation* .., p. 311.

apstrāde ir likumīga tikai tādā apmērā un tikai tad, ja tai ir piemērojams viens no turpmāk minētajiem pamatojumiem:

1) piekrišana;
2) līguma izpilde;
3) juridiskais pienākums;
4) personas vitālās intereses;
5) sabiedrības intereses un likumīgi piešķirtās oficiālās pilnvaras;
6) leģitīmas intereses.

Apstrādes likumīguma princips ir noteikts Policijas direktīvas 8. pantā. Tā 1. punkts paredz, ka apstrāde ir likumīga tikai tad un tiktāl, ciktāl šī apstrāde ir nepieciešama tā uzdevuma izpildei, ko kompetentā iestāde veic 1. panta 1. punktā minētajos nolūkos (proti, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu), un ka tā balstās uz ES vai dalībvalsts tiesībām. Policijas direktīvas 8. panta 2. punkts savukārt paredz, ka dalībvalsts tiesībās, ar ko regulē apstrādi šīs direktīvas darbības jomā, precizē vismaz apstrādes mērķus, apstrādājamos personas datus un apstrādes nolūkus.

Līdzīgi Konvencijas 108+ 5. panta 2. punkts nosaka, ka datu apstrādei jābūt tiesiskajam pamatam: "[k]atra Puse nodrošina, ka datu apstrādi var veikt, pamatojoties uz datu subjekta brīvu, specifisku, informētu un nepārprotamu piekrišanu vai kādu citu tiesisku pamatu, kas noteikts likumā."

VDAR aizliedz biometrisko datu kā īpašas kategorijas personas datu apstrādi, izņemot, ja pastāv kāds no 9. panta 2. punktā noteiktajiem gadījumiem. Šāda atkāpe, piemēram, ir pieļaujama, ja datu subjekts dot nepārprotamu piekrišanu (9. panta 1. punkta a) apakšpunkts). Piekrišanai ir jābūt ne tikai iegūtai atbilstošā veidā, bet tai ir jāatbilst visiem Regulā noteiktiem kritērijiem, proti, tai ir jābūt: brīvai, konkrētai, apzinātai un viennozīmīgai (4. panta 11. punkts).[555] Eiropas Padome Vadlīnijās par sejas atpazīšanu norāda, ka, ņemot vērā prasību pēc šādas datu subjektu piekrišanas, sejas atpazīšanas tehnoloģijas var izmantot tikai kontrolētā vidē verifikācijas, autentifikācijas vai kategorizācijas nolūkos. Biometriskā kategorizācija nozīmē procesu, lai noteiktu, vai indivīda biometriskie dati pieder grupai ar kādām iepriekš definētām īpašībām, un lai veiktu konkrētu darbību. Atkarībā no mērķa īpaša uzmanība jāpievērš datu subjekta "nepārprotamas piekrišanas" kvalitātei, ja tā ir apstrādes tiesiskais pamats.

Lai nodrošinātu brīvu piekrišanu, datu subjektiem jāpiedāvā alternatīvi risinājumi sejas atpazīšanas tehnoloģiju izmantošanai (piemēram, izmantot paroli

555 Sk. Article 29 Data Protection Working Party. (2017). Guidelines on Consent under Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/623051/en

vai identifikācijas zīmi). Turklāt, lai izvēle būtu īsta, tiem ir jābūt viegli izmantojamiem salīdzinājumā ar sejas atpazīšanas tehnoloģiju. Līdzīgi arī Eiropas Datu aizsardzības kolēģija ir uzsvērusi, ka gadījumos, kad piekrišana ir nepieciešama, pārzinis nevar ierobežot piekļuvi saviem pakalpojumiem atkarībā no piekrišanas biometriskai apstrādei, un, ja šādu apstrādi izmanto autentifikācijas nolūkā, datu pārzinim jāpiedāvā alternatīvs risinājums, kas neietver biometrisko apstrādi, – bez ierobežojumiem vai papildu izmaksām datu subjektam.[556]

Eiropas Padome uzsver, ka privātie uzņēmumi nevar izmantot sejas atpazīšanas tehnoloģijas nekontrolētā vidē, piemēram, tirdzniecības centros, it īpaši, lai identificētu interesējošas personas mārketinga vai drošības nolūkā. Iziešanu cauri telpai, kurā tiek izmantotas sejas atpazīšanas tehnoloģijas, nevar uzskatīt par nepārprotamu piekrišanu.[557]

Valsts iestādes nevar izmantot piekrišanu kā tiesisko pamatu, un tām ir atļauts apstrādāt biometriskos datus, ja apstrāde ir vajadzīga "būtisku sabiedrības interešu dēļ", pamatojoties uz ES vai dalībvalsts tiesību aktiem, ja tā ir samērīga ar izvirzīto mērķi, ievēro tiesību uz datu aizsardzību būtību un paredz piemērotus un konkrētus pasākumus datu subjekta pamattiesību un interešu aizsardzībai (VDAR 9. panta 2. punkta g) apakšpunkts).

Policijas direktīvas 10. pants savukārt paredz, ka īpašu kategoriju personas datu apstrāde ir atļauta tikai tad, kad tas ir absolūti nepieciešams, uz to attiecas atbilstošas garantijas attiecībā uz datu subjekta tiesībām un brīvībām, un:

a) tas ir atļauts ES vai dalībvalsts tiesībās;
b) lai aizsargātu datu subjekta vai citas fiziskas personas intereses; vai
c) šāda apstrāde attiecas uz datiem, kurus datu subjekts acīmredzami ir publiskojis.

Konvencija 108+ savukārt paredz, ka biometrisko datu apstrāde, kas unikāli identificē personas, ir atļauta, ja likumā ir paredzēti atbilstoši aizsardzības pasākumi, kas papildina Konvencijas nosacījumus. Šādi aizsardzības pasākumi novērš riskus, ko sensitīvu datu apstrāde var radīt datu subjekta interesēm, tiesībām un pamatbrīvībām, īpaši diskriminācijas risku.

Likumīguma princips un tiesiskā pamata piemērošana ir cieši saistīta ar tiesību uz datu apstrādes ierobežošanas nosacījumiem, kas noteikti, piemēram, Hartas 52. panta 1. punktā, proti, ka tiem ir jābūt paredzētiem likumā, tiem ir jābūt likumīgam mērķim, kā arī nepieciešamiem un proporcionāliem, lai sasniegtu šo mērķi. Konvencijas 108+ 5. pants nosaka datu apstrādes likumību (*legitimacy* – angļu val.) un datu kvalitātes principu. Minētā panta 1. punkts paredz: "Datu apstrāde ir proporcionāla izvirzītajam likumīgajam mērķim un visos apstrādes

556 EDPB (2019), Guidelines 3/2019 on processing of personal data through video devices.

557 Council of Europe (2021), .. Convention 108.

posmos atspoguļo taisnīgu līdzsvaru starp visām attiecīgajām interesēm – gan publiskām, gan privātām – un attiecīgajām tiesībām un brīvībām."

Eiropas Padome Vadlīnijās par sejas atpazīšanu uzsver, ka biometriskā datu apstrāde ar sejas atpazīšanas tehnoloģijām identifikācijas nolūkos kontrolētā vidē, kad biometriskās sistēmas var tikt izmantotas tikai ar personas līdzdalību, kā arī nekontrolētā vidē būtu jāattiecina tikai uz tiesībaizsardzības mērķiem. To drīkst veikt vienīgi kompetentās iestādes drošības jomā. Tiesību akti var paredzēt dažādus nepieciešamības un proporcionalitātes testus atkarībā no tā, vai to mērķis ir verifikācija vai identifikācija, ņemot vērā iespējamos riskus pamattiesībām un kamēr personu attēli tiek likumīgi vākti. Identifikācijas nolūkos ir jāievēro stingra nepieciešamība un proporcionalitāte gan datubāzes (novērošanas saraksta) izveidē, gan (reāllaika) sejas atpazīšanas tehnoloģiju ieviešanā nekontrolētā vidē. Tiesību aktos būtu jāparedz skaidri parametri un kritēriji, kas jāievēro tiesībaizsardzības iestādēm, veidojot datubāzes (novērošanas sarakstus) īpašiem, likumīgiem un nepārprotamiem tiesībaizsardzības mērķiem, piemēram, aizdomām par smagiem pārkāpumiem vai risku sabiedrības drošībai. Ņemot vērā šo tehnoloģiju aizskarošo raksturu, reāllaika sejas atpazīšanas tehnoloģiju ieviešanas posmā nekontrolētā vidē tiesību aktam ir jānodrošina, ka tiesībaizsardzības iestādes pierāda, ka dažādi faktori, tostarp šo tehnoloģiju ieviešanas vieta un laiks, attaisno lietošanas stingru nepieciešamību un proporcionalitāti.[558]

Eiropas Padome jau minētajās vadlīnijās arī pieļauj, ka sejas atpazīšanas tehnoloģijas var izmantot arī citām būtiskām sabiedrības interesēm valsts iestādes, kuru darbība nav saistīta ar tiesībaizsardzības mērķiem. Šādā gadījumā likumdevējiem un lēmumu pieņēmējiem ir jāpieņem īpaši noteikumi par biometrisko apstrādi, kas veikta, izmantojot sejas atpazīšanas tehnoloģijas. Likumdevējiem un lēmumu pieņēmējiem ir jānodrošina, ka nepārprotams un precīzs tiesiskais pamats garantē nepieciešamos aizsardzības pasākumus biometrisko datu apstrādei. Šādam tiesiskam pamatam ir jāietver stingra šo datu izmantošanas nepieciešamība un proporcionalitāte, kā arī jāņem vērā datu subjektu neaizsargātība un vide, kurā šīs tehnoloģijas tiek izmantotas verifikācijas nolūkos. Piemēram, sejas atpazīšanas tehnoloģiju izmantošanu drošības nolūkā kontrolētā vai nekontrolētā vidē, tostarp skolās vai citās sabiedriskās ēkās, parasti nevajadzētu uzskatīt par absolūti nepieciešamu un proporcionālu, ja pastāv mazāk uzmācīgi alternatīvi mehānismi.[559]

Eiropas Padome mudina pieņemt stingru tiesisko regulējumu sejas atpazīšanas tehnoloģiju izmantošanai, norādot arī gadījumus, kad tās nevar izmantot, piemēram, privātie uzņēmumi tās nedrīkstētu lietot nekontrolētā vidē. Tomēr

558 Council of Europe (2021), .. Convention 108.

559 Ibid.

valstīm tiek atstātas plašas iespējas regulēt šo tehnoloģiju izmantošanu publiskā sektorā, lemjot, kad tās būtu atzīstamas par absolūti nepieciešamām un proporcionālām, lai aizsargātu tādas būtiskas sabiedrības intereses kā noziedzīgu nodarījumu izmeklēšana, atklāšana un novēršana, sabiedrības drošība. Eiropas Padomei būtu jānosaka vēl skaidrāki ierobežojumi. Šis jautājums vairāk apskatīts nākamajā nodaļā.

Vēl viens problemātisks aspekts saistībā ar mākslīgā intelekta tehnoloģiju izmantošanu ir par datu, piemēram, fotoattēlu, kas vākti vienam nolūkam, izmantošanu citam nolūkam, piemēram, sejas atpazīšanas datubāzes veidošanai. Lai gan personām varētu nebūt iebildumu pret videonovērošanu drošības nolūkā, ir jānodrošina, ka personas dati netiek izmantoti ļaunprātīgi pilnīgi atšķirīgiem un datu subjektam negaidītiem mērķiem, piemēram, sejas atpazīšanai.

Ar likumīguma principu ir cieši saistīts nolūka ierobežojuma princips, kas ir paredzēts Hartas 8. panta 2. punktā, VDAR 5. (1) (b) pantā, Policijas direktīvas 4. panta 1. punkta b) apakšpunktā un Konvencijas 108+ 5. panta 4. punkta b. apakšpunktā. Tas paredz, ka personas dati tiek vākti konkrētos, skaidros un leģitīmos nolūkos un to turpmāku apstrādi neveic ar minētajiem nolūkiem nesavietojamā veidā. Datu apstrādes nolūks ir jānosaka no paša sākuma, kad dati tiek vākti, un datus turpmāk var apstrādāt noteiktajā nolūkā. Pirms jebkādas turpmākas apstrādes ir jāapsver, vai jaunās apstrādes mērķi ir saderīgi ar sākotnēji definētajiem mērķiem. Pretējā gadījumā jaunajai apstrādei būs nepieciešams noteikts tiesisks pamats.

Saskaņā ar VDAR 6. panta 4. punktu, lai apstrādātu datus citā nolūkā nekā tas, kādā personas dati tika vākti, ir jāsaņem datu subjekta piekrišana, vai arī to var veikt, pamatojoties uz ES vai dalībvalsts tiesību aktiem, kas demokrātiskā sabiedrībā ir vajadzīgs un samērīgs pasākums, lai aizsargātu 23. panta 1. punktā noteiktās svarīgās sabiedrības intereses, piemēram, valsts drošību un aizsardzību, sabiedrisko drošību, noziedzīgu nodarījumu novēršanu, izmeklēšanu un atklāšanu. Citos gadījumos pārzinim ir jāpārliecinās, vai apstrāde citā nolūkā ir savietojama ar nolūku, kādā personas dati sākotnēji tika vākti, cita starpā ņemot vērā

a) jebkuru saikni starp nolūkiem, kādos personas dati ir vākti, un paredzētās turpmākās apstrādes nolūku;
b) kontekstu, kādā personas dati ir vākti, jo īpaši saistībā ar datu subjektu un pārziņa attiecībām;
c) personas datu raksturu, jo īpaši – vai ir apstrādātas īpašas personas datu kategorijas un vai ir apstrādāti personas dati, kas attiecas uz sodāmību un pārkāpumiem;
d) paredzētās turpmākās apstrādes iespējamās sekas datu subjektiem;
e) atbilstošu garantiju esamību, kas var ietvert šifrēšanu vai pseidonimizāciju (VDAR 6. panta 4. punkts).

Policijas direktīvas 4. panta 2. punkts paredz, ka apstrāde, ko veic tas pats vai cits pārzinis, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināLsodus, bet ja šie nolūki nav tie paši, kādos personas dati tika vākti, ir atļauta, ciktāl:

a) pārzinim šādos nolūkos ir atļauts apstrādāt šādus personas datus saskaņā ar ES vai dalībvalsts tiesībām un
b) apstrāde ir vajadzīga un samērīga ar minētajiem citiem nolūkiem saskaņā ar ES vai dalībvalsts tiesībām.

Prasība, lai apstrāde citā nolūkā būtu savietojama ar to iepriekšējās apstrādes nolūku, ir būtiska attiecībā uz sejas atpazīšanas tehnoloģiju izmantošanu kā privātā, tā publiskā sektorā. Eiropas Padome atgādina – ja piekrišana tiek dota konkrētam mērķim, personas datus nevajadzētu apstrādāt veidā, kas nav saderīgs ar šo mērķi. Līdzīgi, ja datus atklāj trešajai personai, arī šādai izpaušanai vajadzētu saņemt īpašu piekrišanu.[560] Jautājums par datu apstrādes mērķa noteikšanu un savietojamību ir aktuāls arī attiecībā uz valsts iestādēm, kas apstrādā datus terorisma vai citu smagu noziedzīgu nodarījumu apkarošanai. Tas ir vispāratzīts nolūks, kas ļauj piekļūt ES un nacionālajām datubāzēm. Izstrādājot informācijas tehnoloģijas sistēmas, tostarp sejas atpazīšanas sistēmas, pastāv risks, ka personas datus (sejas attēlus) var izmantot mērķiem, kas sākotnēji nebija paredzēti, lai apmācītu vai veidotu sejas atpazīšanas tehnoloģijas, prettiesiski piekļūstot liela mēroga datubāzēm, t. i., mērķiem, kādiem šie dati iepriekš nebija paredzēti.[561]

Viens no pašlaik aktuāliem jautājumiem – vai un kādos gadījumos tiesībaizsardzības iestādes var iegūt un izmantot informāciju no sociālo mediju kontiem. Piemēram, tie tika plaši izmantoti, lai sameklētu protestētājus, kas 2021. gada janvārī ielauzās Kapitolija ēkā ASV Vašingtonā.[562] Lai gan VDAR un Policijas direktīva ļauj apstrādāt īpašas kategorijas personas datus, ja datu subjekts tos ir publiskojis (VDAR 9. panta 2. punkta e) apakšpunkts un Policijas direktīvas 10. pants), tomēr tas nenozīmē, ka sejas atpazīšanas tehnoloģijās ir atļauts integrēt personas publicētos sejas attēlus. Eiropas Padome 2021. gadā publicētajās Vadlīnijās par sejas atpazīšanu norāda, ka digitālo attēlu, kas ir augšupielādēti internetā, tostarp sociālajos tīklos vai tiešsaistes fotoattēlu pārvaldības vietnēs, vai kas uzņemti ar videonovērošanas kamerām, izmantošanu nevar uzskatīt par likumīgu tikai tāpēc, ka personas šos datus ir darījušas acīmredzami pieejamus. Likumdevējiem un lēmumu pieņēmējiem ir jānodrošina, ka digitālā formātā, piemēram,

560 Council of Europe (2021), .. Convention 108.

561 FRA (2019), Facial recognition technology.

562 Stone, M., Bartz, D. (8 January, 2021). Some U.S. Capitol rioters fired after internet detectives identify them. *Reuters.* https://www.reuters.com/article/us-usa-election-protests-fallout-idUSKBN29C36M

sociālajos tīklos, pieejamus attēlus nevar apstrādāt, lai iegūtu biometriskās veidnes vai integrētu tās biometriskās sistēmās bez konkrēta tiesiska pamata jaunai apstrādei, kad šie attēli sākotnēji tika uzņemti citiem mērķiem. Tā kā biometrisko veidņu iegūšana no digitālajiem attēliem ietver sensitīvu datu apstrādi, ir jānodrošina tiesiskais pamats, kas dažādās nozarēs un izmantošanas gadījumos atšķiras.[563]

6.2.2. Godprātība un pārredzamība

Tā kā novērošanas tehnoloģijas var izmantot bez jebkādas sadarbības ar datu subjektiem, apstrādes pārredzamība un godprātība (*fairness* – angļu val.) ir ļoti nozīmīgas. Godprātības princips ir vērsts uz godīgām attiecībām starp datu pārzini un datu subjektu un paredz, ka personas dati netiks iegūti negodīgā ceļā un par to neinformējot. Tas nozīmē, ka pārzinis ievēro VDAR noteiktos pienākumus, to skaitā informē datu subjektu par datu apstrādi, izvērtē personas datu apstrādes ietekmi uz datu subjektu un spēj pierādīt apstrādes darbību atbilstību VDAR. Šis princips arī paredz, ka pārzinim pēc iespējas ir jāuzklausa un jāņem vērā datu subjekta vēlmes par viņa datu apstrādi, it īpaši tad, ja datu apstrādes tiesiskais pamats ir piekrišana.[564] Godprātības princips ir cieši saistīts ar pārredzamības principu.

Pārredzamības principa mērķis ir radīt uzticību sistēmām un datu apstrādes procesiem un, ja nepieciešams, tos apstrīdēt.[565] Pārredzamība ir visaptverošs princips, kas attiecas uz trim galvenajām jomām. Tās ir:

1) informācijas sniegšana datu subjektiem saistībā ar godprātīgu apstrādi;
2) datu pārziņa saziņa ar datu subjektiem saistībā ar viņu tiesībām saskaņā ar VDAR; un
3) pārziņa darbība atvieglojot datu subjektiem viņu tiesību izmantošanu.[566]

Godprātīgas un pārredzamas apstrādes principi paredz, ka personas ir jāinformē par novērošanas tehnoloģiju izmantošanu un apstrādes nolūkiem. VDAR 60. apsvērums nosaka: "[..] datu subjekts ir jāinformē par apstrādes darbības esamību un tās nolūkiem." Datu subjekts jāinformē arī par profilēšanas esamību un šādas profilēšanas sekām.

Godprātības un pārredzamības princips rada daudz jaunu jautājumu par mākslīgo intelektu un lielajiem datiem, ņemot vērā sarežģīto datu apstrādi

563 Council of Europe (2021), .. Convention 108.

564 ES Pamattiesību aģentūra, ECT, EP, EDAU (2018), Rokasgrāmata, 118. lpp.

565 Article 29 Data Protection Working Party. (2017). Guidelines on transparency under Regulation 2016/679. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

566 Ibid.

mākslīgā intelekta sistēmās, iznākuma nenoteiktību un mērķu daudzveidību. No minētajiem principiem izriet prasība nodrošināt informāciju par automatizētas lēmumu pieņemšanas esamību un sniegt nozīmīgu informāciju par tā loģiku un paredzamajām sekām, t. i., nodrošināt automatizētu lēmumu izskaidrojamību. Iespējams, ka pārredzamības kā izskaidrojamības ideju var attiecināt arī uz automatizētiem secinājumiem, pat ja konkrēts lēmums vēl nav pieņemts. Pastāv neskaidrība par to, ko nozīmē automatizēta lēmuma loģika un sekas. Attiecībā uz sarežģītu mākslīgā intelekta apstrādi pastāv konflikts starp nepieciešamību sniegt īsu un viegli saprotamu informāciju, no vienas puses, un precīzu un padziļinātu informāciju, no otras puses.

Saistībā ar godprātības principu var runāt arī par automatizētu lēmumu satura godprātīgumu jeb taisnīgumu (*faireness* – angļu val.).[567] VDAR 71. apsvērums nosaka: "Lai nodrošinātu godprātīgu un pārredzamu apstrādi attiecībā uz datu subjektu, ņemot vērā konkrētos apstākļus un kontekstu, kurā personas dati tiek apstrādāti, pārzinim būtu jāizmanto piemērotas matemātiskās vai statistikas procedūras profilēšanai, jāveic atbilstīgi tehniski un organizatoriski pasākumi, lai it īpaši nodrošinātu, ka tiek koriģēti faktori, kuru dēļ rodas personas datu neprecizitātes, un ka līdz minimumam ir samazināts kļūdu rašanās risks, jāgarantē personas datu drošība tādā veidā, lai ņemtu vērā iespējamos riskus attiecībā uz datu subjekta interesēm un tiesībām un lai cita starpā novērstu fizisku personu diskrimināciju dēļ rases vai etniskās izcelsmes, politiskajiem uzskatiem, reliģiskās vai ticības piederības, dalības arodbiedrībā, ģenētiskā vai veselības stāvokļa vai dzimumorientācijas, vai izrietošus pasākumus, kas izraisa šādu diskrimināciju. Automatizēta lēmumu pieņemšana un profilēšana, pamatojoties uz īpašām personas datu kategorijām, būtu jāatļauj tikai saskaņā ar konkrētiem nosacījumiem."

Pārredzamība var paredzēt arī piekļuvi datiem, it īpaši mākslīgā intelekta sistēmu apmācāmajai datu kopai. Piekļuve datiem var būt nepieciešama, lai noteiktu iespējamos netaisnīguma cēloņus, kas izriet no nepietiekamiem vai neobjektīviem datiem vai apmācības algoritma. Tas ir īpaši svarīgi, ja algoritmiskais modelis ir necaurspīdīgs, kā rezultātā, to pārbaudot, nevar atklāt iespējamos trūkumus.[568]

Personas ir jāinformē par riskiem, noteikumiem, aizsardzības pasākumiem un tiesībām saistībā ar personas datu apstrādi un to, kā īstenot savas tiesības saistībā ar šādu apstrādi (VDAR 39. apsvērums). Personām ir jābūt informētām, ka viņu personas datus vāc, izmanto vai citādi apstrādā, un kādā apjomā tie tiek vai

567 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

568 Profilēšanas un automatizētu lēmumu pieņemšanas prasības vairāk apskatītas grāmatas 6.3. nodaļā.

tiks apstrādāti. Pārredzamības principa pamatā ir prasība, ka visa informācija un saziņa, kas saistīta ar personas datu apstrādi, tiek sniegta kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu (VDAR 12. panta 1. punkts, 39., 58. apsvērums). VDAR 12.–14. pants paredz, kādā veidā un kāda informācija ir jāsniedz datu subjektam. VDAR nosaka pārzinim pienākumu sniegt datu subjektam informāciju par personas datu apstrādi, ja dati tiek iegūti no datu subjekta (13. pants)[569], kā arī ja tie nav iegūti no datu subjekta (14. pants). Tomēr pārredzamības principu un informēšanas pienākumu var ierobežot saskaņā ar tiesību aktiem, lai garantētu tiesībaizsardzības mērķus, piemēram, sabiedrības drošību, ievērojot samērīguma principu saskaņā ar VDAR 23. pantu.

Policijas direktīva neparedz pārredzamības principu, un tas var šķist loģiski, jo vairākumā gadījumu sistemātiska pārredzamība kavē noziedzības novēršanas darbību vai valsts iestādes kriminālizmeklēšanas efektivitāti. Tajā pašā laikā Policijas direktīvā kā princips ir paredzēts godprātīga apstrāde (4. panta 1. punkta a) apakšpunkts), un tas var prasīt zināmu pārredzamību. Turklāt 23. apsvērums paredz, ka jebkurai personas datu apstrādei ir jābūt likumīgai, godprātīgai un pārredzamai attiecībā uz personām un jātiek īstenotai tikai konkrētos likumā paredzētos nolūkos. Tas pats par sevi neliedz tiesībaizsardzības iestādēm veikt tādas darbības kā slepena izmeklēšana vai videonovērošana. Šādas darbības var veikt, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu, ja vien šīs darbības ir paredzētas

569 Saskaņā ar VDAR 13. panta 1. punktu, ja pārzinis personas datus vāc no datu subjekta, tam personas datu iegūšanas laikā datu subjektam ir jāsniedz šāda informācija: pārziņa identitāte un kontaktinformācija; attiecīgā gadījumā – datu aizsardzības speciālista kontaktinformācija; apstrādes nolūki, kam paredzēti personas dati un apstrādes juridiskais pamats; pārziņa vai trešās personas leģitīmās intereses, ja apstrāde pamatojas uz šo juridisko pamatu; personas datu saņēmēji vai saņēmēju kategorijas; informācija par datu nosūtīšanu uz trešo valsti vai starptautisku organizāciju un vai tā notiek, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību vai pamatojoties uz atbilstošām garantijām.
VDAR 13. panta 2. punkts paredz, ka papildus minētajai informācijai pārzinis personas datu iegūšanas laikā datu subjektam sniedz arī papildu informāciju, kas vajadzīga, lai nodrošinātu godprātīgu un pārredzamu apstrādi. Šī informācija ir: laikposms, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto laikposma noteikšanai; datu subjekta tiesības saistībā ar apstrādi, piemēram, tiesības piekļūt datiem, ierobežot to apstrādi, dzēst datus, iebilst pret datu apstrādi; tiesības iesniegt sūdzību uzraudzības iestādei; informācija, vai personas datu sniegšana ir noteikta saskaņā ar likumu vai līgumu, vai tā ir priekšnosacījums, lai līgumu noslēgtu, kā arī vai datu subjektam ir pienākums personas datus sniegt un sekas datu nesniegšanas gadījumā; informācija par automatizēta lēmumu pieņemšanu, tai skaitā profilēšanu, un, ja šādi lēmumi rada tiesiskās sekas vai līdzīgā veidā ievērojami ietekmē datu subjektu, vai ietver īpašas personas datu kategorijas, informācija par tajos ietverto loģiku, kā arī apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu.

likumā un ir nepieciešamas un samērīgas demokrātiskā sabiedrībā, pienācīgi ņemot vērā attiecīgās fiziskās personas leģitīmās intereses.

Personas ir jāinformē par riskiem, noteikumiem, garantijām un tiesībām saistībā ar personas datu apstrādi un to, kā īstenot savas tiesības saistībā ar apstrādi. Policijas direktīvas 13. pants nosaka, kāda informācija ir jādara pieejama vai jāsniedz datu subjektam, un 14. pants nosaka datu subjekta piekļuves tiesības.

Konvencijas 108+ 5. panta 4. punkts paredz, ka personas dati ir jāapstrādā taisnīgi un pārredzami. Līdz ar jaunajiem grozījumiem Konvencija 108+ tika papildināta ar 8. pantu, kas nosaka datu apstrādes pārredzamības prasības. Saskaņā ar minētā panta pirmo daļu katra puse nodrošina, ka pārzinis informē datu subjektus par:

a) viņa identitāti un pastāvīgo dzīvesvietu vai uzņēmumu;
b) paredzētās apstrādes tiesisko pamatu un mērķi;
c) apstrādāto personas datu kategorijām;
d) personas datu saņēmējiem vai saņēmēju kategorijām, ja tādas ir; un
e) līdzekļiem, kā izmantot datu subjekta tiesības; kā arī visu nepieciešamo papildu informāciju, lai nodrošinātu personas datu taisnīgu un pārredzamu apstrādi.

Eiropas Padome norāda – ja reāllaika sejas atpazīšanas tehnoloģijas tiek izmantotas nekontrolētā vidē, tiesībaizsardzības iestādes var izmantot slāņveida pieeju, sniedzot nepieciešamo informāciju datu subjektiem, kuri atrodas konkrētajā vietā. Pirmajā informācijas sniegšanas slānī jāsniedz lasāma un saprotama informācija par apstrādes mērķi, iestādi, kas izmanto attiecīgo tehnoloģiju, apstrādes ilgumu un vietu, kurā šī tehnoloģija darbojas, un tā jāpiestiprina atbilstošā tuvumā vietai, kur tā tiek izmantota. Informācijas sniegšanas otrajā slānī jānorāda visa nepieciešamā informācija saskaņā ar Konvencijas 108+ 8. pantu, kas jāizliek pie ieejas vietā, kur tehnoloģija tiek izmantota.[570] Gadījumā, ja tiesībaizsardzības iestādes datubāzes izveidotas identifikācijas vai pārbaudes nolūkā, pārredzamības pienākumu var proporcionāli ierobežot, lai tas neskartu tiesībaizsardzības mērķus saskaņā ar Konvencijas 108+ 11. pantu un ievērojot tās prasības.

Eiropas Padome skaidro, ka faktori, kas nosaka, vai tiek nodrošināta pārredzamība, ietver, piemēram, informācijas sniegšanu personām, vākšanas kontekstu, pamatotas cerības par to, kā dati tiks izmantoti, vai informāciju, ka sejas atpazīšana ir tikai produkta vai pakalpojuma funkcija vai arī tā neatņemama sastāvdaļa. Būtu jāsniedz informācija arī par to, kā sejas atpazīšanas datu vākšana, izmantošana vai koplietošana varētu ietekmēt personas, it īpaši, ja šie dati attiecas uz personām, kuras atrodas neaizsargātās situācijās. Sniegtajai informācijai arī jānorāda, kādas datu subjektam ir tiesības un tiesiskās aizsardzības

570 Council of Europe (2021), .. Convention 108.

līdzekļi.[571] Pārredzamības princips ne tikai nosaka pienākumu informēt konkrētās personas par novērošanas tehnoloģiju izmantošanu un datu apstrādi, bet tas ir arī skatāms plašāk – kā pienākums informēt sabiedrību par šādu tehnoloģiju ieviešanu un izmantošanu, lai veicinātu sabiedrības izpratni un līdzdalību. Šis jautājums aplūkots grāmatas 7.7. nodaļā.

6.2.3. Datu minimizēšana

Datu minimizēšanas princips uzliek pienākumu noteikt minimālo personas datu apjomu, kas nepieciešams konkrētā mērķa sasniegšanai, un neapstrādāt vairāk informācijas, nekā tas ir nepieciešams šim mērķim. VDAR noteiktais datu minimizēšanas princips paredz, ka personas dati ir "adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams to apstrādes nolūkos" (5. panta 1. punkta c) apakšpunkts). Līdzīgi minētais princips ir noteikts Konvencijas 108+ 5. panta 4. punkta c) apakšpunktā. Policijas direktīva arī nosaka, ka dalībvalstis paredz, ka personas dati ir "atbilstīgi, būtiski un nav pārmērīgi, ņemot vērā nolūkus, kādos tos apstrādā" (4. panta 1. punkta c) apakšpunkts).

Mākslīgā intelekta sistēmām parasti ir nepieciešams liels datu apjoms. Dž. Sartors norāda, ka pastāv saspīlējums starp minimizēšanas principu un lielo datu un datu analīzes ideju, kas ietver mākslīgā intelekta un statistikas metožu izmantošanu, lai atklātu jaunas negaidītas korelācijas plašās datu kopās, tomēr šo pretrunu var mazināt. Datu aizsardzības pamatprincipi – īpaši nolūka ierobežošana un datu minimizēšana – jāinterpretē tā, lai tie neizslēgtu personas datu izmantošanu mašīnmācīšanās nolūkos. Tiem nevajadzētu izslēgt algoritmisko modeļu apmācīšanai paredzēto datu kopu (*training sets* – angļu val.) un algoritmisko modeļu izveidi, ja vien mākslīgā intelekta radītās sistēmas ir sociāli izdevīgas un atbilst datu aizsardzības tiesībām.[572]

Datu minimizēšanas princips paredz piemērot proporcionalitātes jeb samērīguma principu, lai iepriekš noteiktos leģitīmos nolūkus īstenotu ar minimāli nepieciešamo datu apjomu. Datu pārzinim ir jāizvērtē, vai konkrētie dati ir nepieciešami noteiktajam nolūkam un vai ir iespējams samazināt apstrādāto datu apjomu. Veidojot mašīnmācīšanās sistēmas, ir jāapsver, vai personas dati ir jāapstrādā konkrētajam mērķim un vai var sasniegt to pašu rezultātu, apstrādājot mazāk datu vai iekļaujot mazāk personu.[573]

571 Council of Europe (2021), .. Convention 108.

572 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

573 ICO (2023). Guidance on AI and data protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

Lai ievērotu minimizēšanas principu, dažos gadījumos ir iespējams samazināt pieejamo datu "personīgumu", nevis datu apjomu, lai datus nevarētu viegli savienot ar indivīdiem, piemēram, izmantojot pseidonimizāciju. Atkārtota identifikācija būtu stingri jāaizliedz, ja vien nav izpildīti visi personas datu tiesiskas vākšanas nosacījumi un ja vien tā ir saderīga ar mērķiem, kādiem dati sākotnēji tika vākti, un pēc tam dati tiek anonimizēti.[574]

Uz personas datu apstrādi dažkārt var attiekties brīvākas minimizēšanas prasības, piemēram, apstrādājot tos statistikai. Tomēr statistikas nolūkā veiktas datu apstrādes beigās nedrīkstētu būt konkrētu personu dati. Informācija, ko izmanto, lai personu pieskaitītu grupai, un ziņas par personas piederību šai grupai, ir personas dati, tātad arī secinātie dati par šo personu. Personas dati ir arī jebkura informācija par cilvēkiem, ko iegūst no datu kopām, lai pieņemtu lēmumus, kas viņus ietekmē, pamatojoties uz grupas profilēšanas informāciju.[575]

6.2.4. Precizitāte

Precizitātes princips uzliek pienākumu nodrošināt, ka "personas dati ir precīzi un, ja vajadzīgs, atjaunināti", kā arī veikt saprātīgus pasākumus, lai nodrošinātu, ka neprecīzi personas dati tiek dzēsti vai laboti (VDAR 5. panta 1. punkta d) apakšpunkts, Policijas direktīvas 4. panta 1. punkta d) apakšpunkts). Arī Konvencijas 108+ 5. panta 4. punkta d) apakšpunkts paredz, ka apstrādājamajiem personas datiem ir jābūt precīziem un, ja nepieciešams, tie regulāri jāatjaunina.

Šis princips attiecas arī uz personas datiem, kas tiek izmantoti, lai apmācītu mākslīgā intelekta algoritmus. Noteiktas grupas locekļus var skart aizspriedumi, ja šo grupu pārstāv tikai ļoti neliela apmācāmās datu kopas apakškopa, jo tas samazinās šīs grupas prognozes precizitāti. It īpaši liels risks ir gadījumā, ja personas dati tiek izmantoti secinājumu izdarīšanai vai lēmumu pieņemšanai par personu.

Vienas no lielākajām bažām attiecībā uz mākslīgā intelekta novērošanas tehnoloģiju izmantošanu ir, ka tās nav pietiekami precīzas. Kļūdaini rezultāti ir saistīti arī ar datu kvalitāti un datu apstrādes precizitāti. Lai nodrošinātu precīzu apstrādi, nepieciešama regulāra novērošanas sarakstā iekļauto sejas attēlu labošana un atjaunināšana. Attiecībā uz kļūdu līmeni jāpatur prātā – algoritms nekad nesniedz precīzu rezultātu, bet tikai varbūtības, piemēram, – 80 % varbūtība, ka novērošanas sarakstā vienā attēlā redzamā persona ir tā pati, kas redzama citā attēlā. Precizitātes novērtējums jāveic dažādām iedzīvotāju grupām, jo vispārējie precizitātes rādītāji var būt maldinoši. Piemēram, sejas atpazīšanas tehnoloģiju

574 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

575 Ibid.

precizitāte var būt atšķirīga atkarībā no personas dzimuma, vecuma un etniskās grupas.[576]

Eiropas Padome vērš uzmanību, ka iestādēm ir jānodrošina, lai biometriskās veidnes un digitālie attēli būtu precīzi un atjaunināti. Piemēram, ir jāpārbauda novērošanas sarakstos ievietoto attēlu un biometrisko veidņu kvalitāte, lai novērstu iespējamu nepatiesu atbilstību, jo zemas kvalitātes attēli var palielināt kļūdu skaitu. Tas ir tieši saistīts ar novērošanas sarakstā apkopoto attēlu avotiem, kas prasa stingri ievērot tādus datu aizsardzības principus kā nolūka ierobežošana. Nepatiesas atbilstības gadījumā iestādēm ir jāveic visi saprātīgie pasākumi, lai nodrošinātu gadījumu atbilstību un digitālo attēlu un biometrisko veidņu precizitāti.[577]

6.2.5. Glabāšanas ierobežojums

Glabāšanas ierobežojuma princips paredz, ka personas dati tiek glabāti veidā, kas pieļauj datu subjektu identifikāciju ne ilgāk, kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā (VDAR 5. panta 1. punkta e) apakšpunkts, Policijas direktīvas 4. panta 1. punkta e) apakšpunkts, Konvencijas 108+ 5. panta 4. punkta e) apakšpunkts). VDAR paredz izņēmumu, ka personas datus var glabāt ilgāk, ciktāl personas datus apstrādā tikai arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos, ar noteikumu, ka tiek īstenoti atbilstoši tehniski un organizatoriski pasākumi, lai aizsargātu datu subjekta tiesības un brīvības (5. panta 1. punkta e) apakšpunkts).

Lai nodrošinātu, ka personas dati netiek glabāti ilgāk, nekā nepieciešams, iestādei ir jānosaka termiņi, kad dati jādzēš, vai periodiski tie ir jāpārskata. Kad personas dati vairs nav nepieciešami noteiktajam nolūkam, tie ir jādzēš vai jāanonimizē.

Termiņš ir jānosaka arī sejas atpazīšanas sistēmās izmantoto biometrisko datu dzēšanai. Eiropas Padome norāda, ka, izmantojot sejas atpazīšanas tehnoloģijas reāllaikā, iestādēm jānodrošina, ka dažādiem apstrādes posmiem tiek piemēroti atšķirīgi glabāšanas periodi. Ja nav konstatēta atbilstība ar biometriskajām veidnēm, to personu datus, kuras iziet cauri nekontrolētai videi, nedrīkst glabāt, un dati ir automātiski jāizdzēš. Savukārt, ja ir konstatēta atbilstība, biometriskās veidnes drīkst glabāt stingri ierobežotu laiku, kā to nosaka tiesību akti, piemērojot nepieciešamos pasākumus. Arī atbilstības pārskatus, kas ietver personas datus, drīkst glabāt ierobežotu laiku. Jebkurā gadījumā novērošanas saraksts un

576 FRA (2019), Facial recognition technology.

577 Council of Europe (2021), .. Convention 108.

biometriskās veidnes ir jādzēš, beidzoties nolūkam, kam tika izmantotas sejas atpazīšanas tehnoloģijas.[578]

6.2.6. Datu drošība

Datu drošības princips ir noteikts VDAR 5. panta 1. punkta f) apakšpunktā (tas tiek saukts par "integritātes un konfidencialitātes principu") un Policijas direktīvas 4. panta 1. punkta f) apakšpunktā, kas paredz, ka personas dati tiek apstrādāti tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus. Līdzīgi datu drošības princips ir noteikts Konvencijas 108+ 7. panta 1. punktā.

Datu drošības princips tālāk konkretizēts VDAR 2. iedaļā (32.–34. pants), kā arī Policijas direktīvas 2. iedaļā (29.–30. pants). Pārzinim un apstrādātājam ir pienākums īstenot atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam. Pārzinim ir pašam jāizvērtē un jānosaka, kādi "atbilstoši pasākumi" ir īstenojami, ņemot vērā tehnikas līmeni (*the state of the art* – angļu val.), īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī riska iespējamību un smaguma pakāpi (VDAR 32. panta 1. punkts, Policijas direktīvas 29. panta 1. punkts). Uz risku balstīta pieeja uzliek pienākumu iestādei novērtēt apstrādei raksturīgos riskus un īstenot atbilstošus tehniskus un organizatoriskus pasākumus, kas būtu piemēroti, lai šos riskus mazinātu un novērstu, ievērojot, ka, jo augstāks ir risks, jo stingrāki ir pasākumi, kas jāveic (VDAR 83. apsvērums).

Datu drošība ir vēl jo svarīgāka, ja tiek apstrādāti biometriskie dati. Tā kā biometriskos datus apstrādā sejas atpazīšanas tehnoloģijas, tās rada ievērojamus drošības riskus, kurus ir grūti vai pat nav iespējams paredzēt. Biometriskos datus, kā pirkstu nospiedumus un sejas attēlus, nevar aizstāt. Ja tie tiek nozagti, tie ir zaudēti pavisam atšķirībā no citiem autentifikācijas veidiem, piemēram, no parolēm, kuras var nomainīt. Tādējādi jebkurš datu drošības pārkāpums var radīt īpaši smagas sekas datu subjektiem. Šādu sensitīvu datu neatļautu izpaušanu nevar labot. Lai aizsargātu sejas atpazīšanas datus un attēlu kopas pret datu pazaudēšanu un neatļautu piekļuvi vai izmantošanu visos apstrādes posmos, neatkarīgi no tā, vai tā ir vākšana, nosūtīšana vai glabāšana, būtu jāīsteno stingri drošības pasākumi gan tehniskā, gan organizatoriskā līmenī. Ir jāveic atbilstoši drošības pasākumi, lai novērstu konkrētajai tehnoloģijai raksturīgus uzbrukumus.

578 Council of Europe (2021), .. Convention 108.

VDAR 32. panta 1. punktā ir uzskaitīti vairāki pasākumi, kas cita starpā var tikt īstenoti:

a) personas datu pseidonimizācija un šifrēšana;
b) spēja nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību;
c) spēja laicīgi atjaunot personas datu pieejamību un piekļuvi gadījumā, ja ir noticis fizisks vai tehnisks negadījums;
d) process regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību.

Arī Policijas direktīva nosaka konkrētas prasības, kuras valstu tiesību aktos ir jāparedz kā pārziņa vai apstrādātāja pienākumi, kas īstenojami pēc risku izvērtēšanas, piemēram, piekļuves kontrole, datu nesēju kontrole, glabāšanas kontrole, lietotāju kontrole, datu piekļuves kontrole, komunikācijas kontrole, datu ievades kontrole, spēja atjaunot uzstādītās sistēmas ("atgūšana"), spēja nodrošināt, ka sistēma funkcionē tā, ka par tās darbības kļūdu parādīšanos tiek ziņots ("drošums") un ka saglabātie dati nevar tikt sabojāti sistēmas darbības traucējumu dēļ ("integritāte") (29. panta 2. punkts).

Par personas datu aizsardzības pārkāpumu pārzinim ir pienākums ziņot uzraudzības iestādei (VDAR 33. pants, Policijas direktīvas 30. pants), kā arī datu subjektam (VDAR 34. pants, Policijas direktīvas 31. pants). Konvencija 108+ arī paredz pienākumu pārzinim nekavējoties ziņot vismaz kompetentajai uzraudzības iestādei par datu pārkāpumiem, kas var nopietni traucēt datu subjektu tiesības un pamatbrīvības (7. panta 2. punkts).

Pārzinim ir jāziņo par pārkāpumu uzraudzības iestādei "bez nepamatotas kavēšanās, un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms" (VDAR 33. panta 1. punkts, Policijas direktīvas 30. panta 1. punkts). Izņēmums, kad pārzinis var neziņot par pārkāpumu uzraudzības iestādei, ir gadījumā, ja maz ticams, ka tas varētu radīt risku fizisku personu tiesībām un brīvībām.

Pārzinim ir pienākums ziņot par pārkāpumu arī datu subjektam, tomēr tikai gadījumā, ja pārkāpums varētu radīt augstu risku fizisku personu tiesībām un brīvībām (VDAR 34. panta 1. punkts, Policijas direktīvas 31. panta 1. punkts). Paziņojums datu subjektam nav jāsniedz, ja pārzinis izpildījis vienu no trim nosacījumiem:

1) ir īstenojis atbilstīgus tehniskus un organizatoriskus aizsardzības pasākumus, un šie pasākumi ir piemēroti personas datiem, ko skāris pārkāpums, jo īpaši tas attiecas uz tādiem pasākumiem, kas personas datus padara nesaprotamus personām, kurām nav pilnvaru piekļūt personas datiem, piemēram, šifrēšana;

2) ir veicis pasākumus, lai, visticamāk, vairs nepastāvētu risks attiecībā uz datu subjektu tiesībām un brīvībām;
3) ja tas pārzinim prasītu nesamērīgi lielas pūles; šādā gadījumā pārzinis var izmantot publisku saziņu vai līdzīgu pasākumu, ar ko datu subjekti tiek informēti vienlīdz efektīvā veidā (VDAR 34. panta 3. punkts, Policijas direktīvas 31. panta 3. punkts).

Eiropas Padome Sejas atpazīšanas vadlīnijās arī vērš uzmanību, ka par visiem datu drošības pārkāpumiem, kas var nopietni ietekmēt datu subjektu tiesības un pamatbrīvības, jāziņo uzraudzības iestādei un attiecīgā gadījumā datu subjektiem. Drošības pasākumiem vajadzētu attīstīties laika gaitā, reaģējot uz mainīgajiem draudiem un konstatētajām ievainojamībām. Tiem jābūt samērīgiem arī ar datu sensitivitāti, kontekstu, kurā tiek izmantota īpaša sejas atpazīšanas tehnoloģija, un ar datu izmantošanas mērķiem, kaitējuma iespējamību indivīdiem un citiem būtiskiem faktoriem. Stingra sejas atpazīšanas datu glabāšanas un iznīcināšanas prakse, izmantojot drošas procedūras un ievērojot pēc iespējas īsāku datu glabāšanas periodu, arī palīdz samazināt drošības draudus.[579]

Tiek veikti arvien jauni pētījumi par mākslīgā intelekta tehnoloģijām, meklējot veidus, kā aizsargāt biometrisko datu drošību. Nozares labā prakse var atvieglot drošības prasību ieviešanu, sniedzot norādes un ieteikumus, kā identificēt un novērtēt riskus un kādi pasākumi būtu ieviešami, lai mazinātu drošības riskus.[580]

6.2.7. Pārskatatbildība

Pārskatatbildības princips (*accountability* – angļu val.) paredz, ka pārzinis ir atbildīgs par visu iepriekš minēto datu aizsardzības pamatprincipu ievērošanu un "var to uzskatāmi pierādīt" (VDAR 5. panta 2. punkts, Policijas direktīvas 4. panta 4. punkts). Pārzinim ir jāvar uzskatāmi parādīt jeb pierādīt atbilstību visām datu aizsardzības prasībām, veicot "atbilstošus tehniskus un organizatoriskus pasākumus", ņemot vērā "apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisko personu tiesībām un brīvībām" (VDAR 24. panta 1. punkts, Policijas direktīvas 24. pants).

Pārskatatbildības princips uzliek pienākumu īstenot "atbilstošus tehniskus un organizatoriskus pasākumus", lai uzskatāmi parādītu, ka apstrādē tiek ievērotas visas datu aizsardzības prasības, kas paredzētas tam piemērojamā tiesiskajā

579 Council of Europe (2021), .. Convention 108.

580 Sk., piemēram, ICO. How should we assess security and data minimisation in AI? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/; ENISA. (2017). Handbook on Security of Personal Data Processing. https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

regulējumā. Pārzinis ir atbildīgs par datu apstrādes likumību, datu subjektu tiesību garantēšanu, datu drošības un citu prasību izpildi. Atbilstība var tikt demonstrēta, veicot dažādus pasākumus, tostarp: informējot datu subjektus par datu apstrādi (VDAR 13. pants); uzturot datu subjektu tiesību īstenošanas kārtību un procedūras, piemēram, piekļuves, labošanas un dzēšanas pieprasījumus (VDAR 12., 24. pants); īstenojot datu drošības pasākumus (VDAR 32. pants); uzturot personas datu apstrādes darbības reģistru (30. pants); veicot novērtējumu par ietekmi uz datu aizsardzību (VDAR 25. pants); nozīmējot datu aizsardzības speciālistu (VDAR 37. pants); noslēdzot personas datu apstrādes līgumu (VDAR 28. panta 3. punkts); sadarbojoties ar uzraudzības iestādi; pievienojoties rīcības kodeksam un sertificējot personas datu apstrādes darbības (VDAR 40., 42. pants); pieņemot vadlīnijas un procedūras; izglītojot un apmācot darbiniekus par datu aizsardzību; īstenojot pārbaudes procedūras (iekšējo un ārējo auditu).[581] Lai gan pārskatatbildības princips VDAR nav tieši attiecināts uz apstrādātāju, arī apstrādātājam ir pienākums pierādīt tam noteikto prasību izpildi, piemēram, vai ir noslēgts līgums ar datu pārzini (VDAR 28. panta 3. punkts).

Lai īstenotu pārskatatbildības principu, būtiska loma ir datu aizsardzības speciālista nozīmēšanai, kas ir obligāta prasība visām valsts iestādēm. Privātiem uzņēmumiem ir jāizvērtē, vai tiem ir pienākums to nozīmēt, kā arī to var darīt brīvprātīgi. Saskaņā ar Policijas direktīvas 32. pantu dalībvalstis paredz, ka pārzinis ieceļ datu aizsardzības speciālistu.

VDAR 37. panta 1. punkts nosaka pārziņiem un apstrādātājiem pienākumu iecelt datu aizsardzības speciālistu šādos trīs gadījumos:

1) apstrādi veic publiska iestāde vai struktūra;
2) pārziņa vai apstrādātāja pamatdarbība sastāv no apstrādes darbībām, kurām nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā;
3) pārziņa vai apstrādātāja pamatdarbības ietver īpašo kategoriju datu apstrādi vai personas datu par sodāmību un pārkāpumiem apstrādi plašā mērogā.

Ja tiek izmantotas tehnoloģijas, kas ietver biometrisko datu apstrādi, ir obligāti jāieceļ datu aizsardzības speciālists. VDAR nav definēts, ko nozīmē "plašs mērogs" un "regulāra un sistemātiska novērošana", bet to piemērošanu ir skaidrojusi 29. panta darba grupa.[582] Datu subjektu regulāra vai sistemātiska novērošana

581 Sk., piemēram, ICO, How should we assess security and data minimisation in AI?; ENISA (2017), Handbook on Security of Personal Data Processing.

582 Article 29 Data Protection Working Party. (2016). Guidelines on Data Protection Officers ('DPOs'). https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

ir, piemēram, profilēšana un vērtēšana, mērķorientētas reklāmas, atrašanās vietas izsekošana ar mobilās lietotnes starpniecību, fiziskās sagatavotības un veselības datu novērošana ar valkājamu ierīču starpniecību u. tml.

Datu aizsardzības speciālistu ieceļ, pamatojoties uz viņa profesionālo kvalifikāciju, jo īpaši speciālām zināšanām datu aizsardzības tiesību un prakses jomā un spēju pildīt speciālista uzdevumus (VDAR 37. panta 5. punkts). VDAR neizvirza konkrētākas profesionālās kvalifikācijas prasības.

FPDAL paredz, ka par datu aizsardzības speciālistu var iecelt personu, kura ir iekļauta Datu valsts inspekcijas datu aizsardzības speciālistu sarakstā vai cita persona (17. pants). Datu aizsardzības speciālistu sarakstā ir iekļauti speciālisti, kuri ir nokārtojuši DVI organizēto datu aizsardzības speciālistu kvalifikācijas eksāmenu (18.–19. pants). Tomēr pārzinim vai apstrādātājam ir iespēja iecelt par speciālistu arī citu personu, kas var apliecināt savu profesionālo kvalifikāciju citādā veidā.

Mākslīgā intelekta un citu informācijas sistēmu, produktu un pakalpojumu, kas balstās vai ietver personas datu apstrādi, izstrādei ir jābalstās uz integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principiem. Integrēta datu aizsardzība ietver dažādus atbilstošus tehniskus un organizatoriskus pasākumus, kurus pārzinis veic gan apstrādes līdzekļu noteikšanas, gan pašas apstrādes laikā, lai īstenotu datu aizsardzības principus un apstrādē integrētu vajadzīgās garantijas, lai ievērotu datu aizsardzības prasības un aizsargātu datu subjektu tiesības (VDAR 25. panta 1. punkts, Policijas direktīvas 20. pants). Lai nodrošinātu atbilstību minētajam principam, pārzinim ir jāizvērtē datu apstrādes darbību un sistēmu atbilstība datu aizsardzības prasībām un jāveic atbilstoši pasākumi, lai nodrošinātu datu aizsardzību un drošību. Šādi pasākumi var ietvert, piemēram, apstrādāto personas datu daudzuma samazināšanu, personas datu pseidonimizāciju, tiklīdz tas ir iespējams, pārredzamību attiecībā uz funkcijām un personas datu apstrādi, kas datu subjektam dod iespēju pārraudzīt datu apstrādi un pārzinim dod iespēju izveidot un uzlabot drošības pasākumus (VDAR 78. apsvērums).

Integrēta datu aizsardzība aptver visus sejas atpazīšanas tehnoloģiju datu apstrādes posmus. Uzņēmumiem, kas izmanto šīs tehnoloģijas identifikācijas vai verifikācijas nolūkos, ir jānodrošina, ka viņu izmantotie produkti vai pakalpojumi ir paredzēti biometrisko datu apstrādei saskaņā ar nolūka ierobežošanas, datu minimizēšanas un ierobežota uzglabāšanas ilguma principiem un jāintegrē visi pārējie nepieciešamie drošības pasākumi tehnoloģijās. Kad organizācijas nosaka šo tehnoloģiju tehniskās iezīmes, tām ir jāievieš šie principi savā projektā, lai nodrošinātu, ka to ieviešana atbilst tiesībām uz datu aizsardzību.[583]

583 Council of Europe (2021), .. Convention 108.

Princips datu aizsardzībai pēc noklusējuma paredz – pārzinis īsteno atbilstošus tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka pēc noklusējuma tiek apstrādāti tikai tādi personas dati, kas ir nepieciešami katram konkrētajam apstrādes nolūkam. Minētais pienākums attiecas uz vākto personas datu apjomu, to apstrādes pakāpi, glabāšanas laikposmu un to pieejamību. Īpaši svarīgi ir nodrošināt, ka pēc noklusējuma pārzinis personas datus bez personas līdzdalības nedara pieejamus nenoteiktam personu skaitam (VDAR 25. panta 2. punkts, Policijas direktīvas 20. panta 2. punkts).

Sistēmu izstrādātāji, programmatūras inženieri, informācijas drošības speciālisti un citas izstrādes procesā iesaistītās personas var izmantot uzraudzības iestāžu[584] un citu organizāciju, piemēram, ENISA[585], izdotās vadlīnijas par integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principu piemērošanu. Datu aizsardzības ekspertu iesaistīšana komandās, kas strādā pie tehnoloģijas izstrādes, kā arī datu aizsardzības prasību izvirzīšana tehniskajā specifikācijā palīdz nodrošināt datu aizsardzības pēc noklusējuma principa ievērošanu.[586]

Atbildības princips paredz, ka organizācijas īsteno atbilstīgu personas datu pārvaldības politiku, ciktāl tas ir samērīgi ar apstrādes darbībām. Minētie pasākumi ietver arī iekšējo procedūru (piemēram, personas datu aizsardzības politikas, informācijas sistēmu drošības politikas utt.) pieņemšanu un ieviešanu praksē, atbildīgo personu nozīmēšanu, regulāru apmācību veikšanu, lai ieviestu datu aizsardzības standartus organizācijas kultūrā. Pārzinim ir jāizstrādā un jāsaglabā dokumentācija, lai varētu gan datu subjektam, gan uzraudzības iestādei parādīt, kādus atbilstības pasākumus tas ir veicis.[587]

Konvencijas 108+ 10. pants nosaka, ka valstis nodrošina, ka pārziņi un attiecīgā gadījumā apstrādāji veic visus nepieciešamos pasākumus, lai izpildītu konvencijas saistības un lai saskaņā ar valstu tiesību aktiem varētu pierādīt, it īpaši uzraudzības iestādei, ka viņu veiktā datu apstrāde atbilst konvencijas noteikumiem.

Eiropas Padome norāda, ka, izmantojot sejas atpazīšanas tehnoloģijas, ir jāveic organizatoriski pasākumi. Tie ir:

584 Sk., piemēram, ICO. Data protection by design and by default. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

585 ENISA. (2016). Privacy Enhancing Technologies: Evolution and State of the Art, A Community Approach to PETs Maturity Assessment. https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art

586 FRA (2019), Facial recognition technology.

587 Sk. Article 29 Data Protection Working Party. (2010). Opinion 3/2010 on the principle of accountability. http://www.dataprotection.ro/servlet/ViewDocument?id=654

- pārredzamas politikas, procedūru un prakses īstenošana, lai nodrošinātu, ka sejas atpazīšanas tehnoloģiju pamatā ir datu subjektu tiesību aizsardzība;
- pārredzamības ziņojumu publicēšana par sejas atpazīšanas tehnoloģiju konkrētu izmantošanu;
- apmācības programmu un revīzijas procedūru izveidošana un nodrošināšana tiem, kas ir atbildīgi par sejas atpazīšanas datu apstrādi;
- iekšējās uzraudzības komitejas izveidošana, lai izvērtētu un apstiprinātu jebkādu apstrādi, kas saistīta ar sejas atpazīšanas datiem;
- piemērojamo prasību attiecināšana uz trešo personu pakalpojumu sniedzējiem, biznesa partneriem vai citām personām, kas izmanto sejas atpazīšanas tehnoloģiju (un piekļuves liegšana trešajām personām, kas tām neatbilst);
- publiskajā sektorā: iepriekšējas novērtēšanas ierobežojumu noteikšana publiskā iepirkuma procedūrās, iesaistot sejas atpazīšanas rīku piegādātājus, un minimālā darbības līmeņa novērtēšana attiecībā uz precizitāti, it īpaši attiecībā uz tiesībaizsardzības mērķiem.

Iestādēm un organizācijām, kas izmanto sejas atpazīšanas tehnoloģijas, ir jāveic nepieciešamie tehniskie pasākumi, lai nodrošinātu biometrisko datu kvalitāti, ievērojot starptautiski saskaņotus tehniskos standartus atkarībā no to izmantošanas konteksta. Tām ir jānodrošina, lai cilvēku pārraudzībai joprojām būtu izšķiroša nozīme, ja tiek veiktas darbības, kas balstās uz šo tehnoloģiju rezultātiem. Tas prasa ieviest organizatoriskos pasākumus, lai uzraudzītu, kā tiek pieņemti lēmumi, kas var būtiski ietekmēt indivīdus.[588]

6.3. Automatizēta lēmumu pieņemšana un cilvēka līdzdalības prasība

Mākslīgā intelekta sistēmas, kas balstās uz lielu datu apjomu, ļauj pieņemt automatizētus lēmumus, kas arvien plašāk tiek izmantoti arī publiskajā sektorā, to skaitā ir lēmumi, kas pieņemti, izmantojot novērošanas tehnoloģijas un prognozējošos algoritmus sabiedrības drošības un noziedzības apkarošanas interesēs. Grāmatā iepriekš jau minēts, ka sejas atpazīšanas tehnoloģiju algoritmi nekad nenodrošina pilnīgi precīzu rezultātu, bet gan tikai varbūtības. Lai gan šīs tehnoloģijas precizitāte arvien palielinās, vienmēr pastāv noteikts kļūdu līmenis, līdz ar to automatizētu rezultātu piemērošana var negatīvi ietekmēt personu, it

588 Council of Europe (2021), .. Convention 108.

īpaši, ja uz šo rezultātu pamata tiek pieņemts lēmums, kas rada personai negatīvas sekas.

Cilvēka virsvadība ir jauna prasība, kas ietverta MI akta priekšlikumā. Tā paredz, ka mākslīgā intelekta sistēmas lietošanas laikā fiziskai personai ir jāvar to efektīvi pārraudzīt, un tas nozīmē: spēju pilnībā izprast sistēmas iespējas un ierobežojumus; apzināties tendenci automātiski vai pārmēru paļauties uz mākslīgā intelekta sistēmas radītajiem iznākumiem (piemēram, sniedzot ieteikumu, kādu lēmumu pieņemt); spēju pareizi interpretēt augsta riska mākslīgā intelekta sistēmas radītos iznākumus; spēju izlemt nelietot mākslīgā intelekta sistēmu vai citādi neievērot sistēmas darbības iznākumu; spēju iejaukties sistēmas darbībā vai pārtraukt to katrā atsevišķā situācijā; spēju iejaukties augsta riska mākslīgā intelekta sistēmas darbībā vai pārtraukt to, izmantojot pogu "stop" vai līdzīgu procedūru (14. panta 4. punkts).[589] Turklāt attiecībā uz augsta riska sistēmām, ko paredzēts izmantot fizisku personu tālidentifikācijai reāllaikā un vēlāklaikā (III pielikuma 1. punkta a) apakšpunkts), jānodrošina, ka lietotājs turklāt neveic nekādas darbības vai nepieņem nekādu lēmumu, pamatojoties uz identifikāciju, kas izriet no attiecīgās sistēmas, ja to nav pārbaudījušas un apstiprinājušas vismaz divas fiziskas personas (MI akta priekšlikuma 14. panta 5. punkts). Cilvēka virsvadības prasība paredz cilvēka līdzdalību automatizētu lēmumu pieņemšanas gadījumā.

Lēmuma pieņemšana ir pilnībā automatizēta, kad tā notiek bez cilvēka līdzdalības. Automatizētu lēmumu pieņemšana var daļēji pārklāties vai notikt profilēšanas rezultātā, un to var veikt gan ar, gan bez profilēšanas. Arī profilēšana var notikt bez automatizētu lēmumu pieņemšanas.[590]

Profilēšana ir jebkura veida automatizēta personas datu apstrāde, kas izpaužas kā personas datu izmantošana nolūkā izvērtēt konkrētus ar fizisku personu saistītus personiskus aspektus, jo īpaši – analizēt vai prognozēt aspektus saistībā ar minētās fiziskās personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos (VDAR 4. panta 4. punkts).

Pastāv trīs iespējamie veidi, kā var izmantot profilēšanu. To var izmantot:

1) vispārīgai profilēšanai bez automatizētu lēmumu pieņemšanas;
2) lēmumu pieņemšanai, pamatojoties uz profilēšanu;
3) tikai automatizēta lēmumu pieņemšanai, tostarp profilēšanai, kas rada tiesiskas sekas vai līdzīgā veidā ievērojami ietekmē datu subjektu.[591]

589 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

590 Article 29 Data Protection Working Party. (2017, as last revised and adopted 2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/612053

591 Ibid.

Datu subjektam ir tiesības nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde, tostarp profilēšana, kas attiecībā uz datu subjektu rada tiesiskās sekas vai kas līdzīgā veidā ievērojami ietekmē datu subjektu (VDAR 22. panta 1. punkts, Policijas direktīvas 11. panta 1. punkts). Tomēr no šī aizlieguma ir pieļaujami izņēmumi. Saskaņā ar VDAR 21. panta 2. punktu izņēmuma kārtā šāds lēmums var tikt pieņemts, ja tas

1) ir vajadzīgs, lai noslēgtu vai izpildītu līgumu starp datu subjektu un datu pārzini;
2) pamatojas uz datu subjekta nepārprotamu piekrišanu; vai
3) ir atļauts saskaņā ar ES vai dalībvalsts tiesību aktiem, kuri ir piemērojami pārzinim un kuros ir arī noteikti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības, un leģitīmās intereses.

Pirmajos divos gadījumos datu pārzinim jāveic atbilstīgi pasākumi, lai aizsargātu datu subjekta tiesības un brīvības, un leģitīmās intereses – vismaz tiesības panākt cilvēka līdzdalību no pārziņa puses –, lai datu subjekts varētu paust savu viedokli un apstrīdēt lēmumu. Tomēr minētie lēmumi nevar tikt pamatoti ar īpašām personas datu kategorijām, izņemot, ja datu subjekts ir devis nepārprotamu piekrišanu vai apstrāde ir vajadzīga būtisku sabiedrības interešu dēļ, pamatojoties uz ES vai dalībvalsts tiesību aktiem, un tiek nodrošināti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības, un leģitīmās intereses (VDAR 21. panta 3. punkts).

Policijas direktīvas 11. panta 1. punkts nosaka – dalībvalstis paredz, ka lēmums, kas balstās tikai uz automātisku apstrādi, tostarp uz profilēšanu, un kas rada nelabvēlīgas juridiskas sekas attiecībā uz datu subjektu vai būtiski viņu ietekmē, ir aizliegts, ja vien tas nav atļauts ES vai dalībvalsts tiesībās, kurās ir paredzētas atbilstošas garantijas attiecībā uz datu subjekta tiesībām un brīvībām, vismaz attiecībā uz tiesībām panākt cilvēka iejaukšanos no pārziņa puses. Līdzīgi kā VDAR, Policijas direktīva arī paredz, ka automatizētus individuālus lēmumus nepamato ar īpašām personas datu kategorijām, tostarp biometriskajiem datiem, izņemot, ja tiek nodrošināti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības, un leģitīmās intereses (Policijas direktīvas 11. panta 2. punkts). Turklāt šī direktīva paredz būtisku nosacījumu, ka profilēšana, kas izraisa diskrimināciju pret fiziskām personām, pamatojoties uz īpašu kategoriju personas datiem, ir aizliegta saskaņā ar ES tiesībām (Policijas direktīvas 11. panta 3. punkts).

Aizsardzības pasākumi automatizētu lēmumu pieņemšanas gadījumā, it sevišķi tad, ja tiek apstrādāti biometriskie dati, ir šādi: tiesības apstrīdēt lēmumu; tiesības panākt cilvēka līdzdalību; tiesības būt informētam par to, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana; tiesības saņemt jēgpilnu informāciju par automatizētajā lēmumā ietverto loģiku, kā arī šādas apstrādes

nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu (VDAR 13. panta 2. punkta f) apakšpunkts, 14. a 2. punkta f) apakšpunkts).

Minētās normas paredz informēšanas pienākumu, un tās ir bijušas plašu diskusiju centrā, kur šī juridiskā prasība ir bijusi saistīta ar vispārīgāku un fundamentālu jautājumu par mākslīgā intelekta sistēmu un to rezultātu, kā arī ar to saistīto cilvēka pieņemto lēmumu izskaidrojamību (*explainability* – angļu val.).[592] Mākslīgā intelekta sistēmas un to lēmumi ir jāizskaidro. Cilvēkiem arī jāapzinās, ka viņi mijiedarbojas ar mākslīgā intelekta sistēmu. Pārredzamības prasība paredz, ka ir jāinformē par mākslīgā intelekta sistēmu iespējām un mērķiem, kā arī ierobežojumiem. Cilvēkiem ir jāsaprot, kā tiek izstrādātas, apmācītas un izmantotas mākslīgā intelekta sistēmas. Izskaidrojamība attiecas uz spēju izskaidrot gan sistēmas tehniskos procesus, gan ar tiem saistītos pieņemtos lēmumus. Tehniskā izskaidrojamība prasa, lai mākslīgā intelekta sistēmas pieņemtos lēmumus varētu saprast cilvēki. Pārredzamības prasības var atklāt, kā šīs sistēmas tiek izmantotas, lai veiktu prognozes, sniegtu ieteikumus vai pieņemtu lēmumus. Tās var atklāt kritērijus, kas ietekmē konkrētu prognozi vai lēmumu. Parasti šī prasība neparedz noteikta koda vai datu koplietošanu, jo tādējādi varētu tikt atklāts komercnoslēpums vai sensitīvi lietotāja dati. Tomēr daudzos gadījumos mākslīgā intelekta sistēmas ir pārāk sarežģītas, lai tās varētu izskaidrot. Ne vienmēr ir iespējams izskaidrot, kāpēc mākslīgā intelekta sistēma ir pieņēmusi konkrētu rezultātu vai lēmumu un kāda ievades faktoru kombinācija to veicināja. Šos gadījumus dēvē par "melno kasti" (*black box* – angļu val.), un to vietā varētu izmantot citus izskaidrojamības pasākumus, piemēram, izsekojamību, auditējamību un pārredzamu informāciju par sistēmas iespējām.

Līdzās informēšanai vēl viena būtiska garantija ir tiesības apstrīdēt automatizētus lēmumus. Atšķirībā no VDAR 22. panta 3. punkta Policijas direktīvā nav tieši noteiktas tiesības apstrīdēt automatizētus lēmumus, bet šīs tiesības ir pieminētas 38. apsvērumā, kur norādīts, ka katrā ziņā uz šādu apstrādi būtu jāattiecina atbilstošas garantijas, tostarp īpašas informācijas sniegšana datu subjektam un tiesības panākt cilvēka iejaukšanos, jo īpaši – paust savu viedokli, saņemt paskaidrojumu par lēmumu, kas pieņemts pēc šādas izvērtēšanas, un apstrīdēt lēmumu.

Konvencija 108+ arī nosaka personas tiesības nebūt tāda lēmuma subjektam, kas viņu būtiski ietekmē un kas pamatojas tikai uz automatizētu datu apstrādi, neņemot vērā viņa viedokli. Izņēmums, ja šāds lēmums ir atļauts ar tiesību aktu, kurā noteikti arī piemēroti pasākumi, lai aizsargātu datu subjekta tiesības,

592 Sk., piemēram, Barredo Arrieta, et al. (2020), Explainable Artificial Intelligence ..; Hamon, R., Junklewitz, H. and Sanchez, M. J. (2020). Robustness and Explainability of Artificial Intelligence. Publications Office of the European Union, Luxembourg. http://dx.doi.org/10.2760/57493; Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

brīvības un likumīgās intereses (9. panta 1. punkta a) apakšpunkts, 9. panta 2. punkts).

Eiropas Padome skaidro – ja sejas atpazīšanas tehnoloģiju izmantošana ir paredzēta, lai lēmumu varētu pieņemt, tikai un vienīgi pamatojoties uz automatizētu apstrādi, kas būtiski ietekmētu datu subjektu, datu subjektam it īpaši jābūt tiesībām, lai šāda apstrāde netiktu veikta bez viņa viedokļa uzklausīšanas. Ja, izmantojot reāllaika sejas atpazīšanas tehnoloģijas, personas vadās tikai pēc šo tehnoloģiju rezultātiem, to var uzskatīt par tikai automatizētu lēmumu pieņemšanu, kas iespējamās viltus sakritības dēļ var būtiski ietekmēt datu subjektu. Datu subjekts var pieprasīt, lai tiktu ņemts vērā viņa viedoklis.[593]

Svarīga prasība attiecībā uz tādu tehnoloģiju kā sejas atpazīšana izmantošanu ir tā, ka ikvienā gadījumā ir jānodrošina cilvēka iejaukšanās. Tas nozīmē, ka sakritības, kas tiek konstatētas ar šo tehnoloģiju, ir jāizvērtē, piemēram, policistam, kurš pārbaudīs šo sakritību un atbilstoši rīkosies. Šajā posmā jau tiek izslēgti daudzi viltus pozitīvi rezultāti.[594]

Jēdziens "automatizēta lēmumu pieņemšana" nav līdz galam skaidrs. Dažos gadījumos cilvēka iejaukšanās var būt vienkārši visu sistēmas rezultātu apstiprināšana, un tādējādi šis lēmums būs faktiski automatizēts. Būtu jāvērtē arī pretējie gadījumi, kad cilvēki pārskata un potenciāli atceļ sistēmas rezultātus. Pētījumi liecina, ka cilvēki atceļ algoritmu rezultātus galvenokārt tad, ja rezultāts atbilst viņu stereotipiem, un tā rezultātā, piemēram, mazākumtautību grupas var tikt nostādītas neizdevīgā stāvoklī. Šāda rīcība apdraud automatizētās apstrādes iespējamo pievienoto vērtību, jo tā var būt precīzāka vai atsevišķos gadījumos pat taisnīgāka.[595]

Vēl viena prasība, kas nav tieši noteikta VDAR, Policijas direktīvā un Konvencijā 108+, ir, ka lēmumam ir jābūt "saprātīgam" (*reasonable* – angļu val.). Tas nozīmē, ka lēmuma pieņemšanas mērķi ir atbalstāmi un izmantotās metodes ir uzticamas.[596]

6.4. Datu subjekta tiesības

ES datu aizsardzības regulējums datu subjektam paredz plaša apjoma tiesības:

- tiesības uz informāciju (VDAR 13., 14. pants, Policijas direktīvas 13. pants);
- piekļuves tiesības (VDAR 15. pants, Policijas direktīvas 14., 15. pants);

593 Council of Europe (2021), .. Convention 108.

594 FRA (2019), Facial recognition technology.

595 Ibid.

596 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

- tiesības labot datus (VDAR 16. pants, Policijas direktīvas 16. panta 1. punkts);
- tiesības dzēst datus (VDAR 17. pants, Policijas direktīvas 16. panta 2. punkts);
- tiesības ierobežot apstrādi (VDAR 18. pants, Policijas direktīvas 16. panta 3. punkts);
- tiesības uz datu pārnesamību (VDAR 20. pants);
- tiesības iebilst pret datu apstrādi (VDAR 21. pants);
- tiesības nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde, tostarp profilēšana (VDAR 22. pants, Policijas direktīvas 21. pants).

Līdzīgas tiesības datu subjektam paredz arī Konvencijas 108+ 9. pants:

a) tiesības nebūt automatizēta lēmuma subjektam;
b) tiesības saņemt apstiprinājumu par datu apstrādi, kas attiecas uz šo personu, saņemt informāciju saprotamā formā par apstrādātajiem datiem, to izcelsmi, saglabāšanas periodu, kā arī jebkuru citu informāciju, kas pārzinim jāsniedz, lai nodrošinātu datu apstrādes pārredzamību;
c) tiesības saņemt informāciju par datu apstrādes pamatojumu (*reasoning* – angļu val.), ja attiecībā uz personu tiek piemēroti šādas apstrādes rezultāti;
d) tiesības iebilst pret personas datu apstrādi, ja vien pārzinis nepierāda, ka tā tiesiskais pamatojums apstrādāt datus ir svarīgāks par personas interesēm vai tiesībām un pamatbrīvībām;
e) tiesības labot vai dzēst datus, ja tie tiek apstrādāti pretrunā ar konvencijas noteikumiem;
f) tiesības saņemt tiesiskās aizsardzības līdzekļus, ja ir pārkāptas personas tiesības saskaņā ar minēto konvenciju;
g) tiesības lūgt uzraudzības iestādes palīdzību, izmantojot savas tiesības.

Tā kā sejas atpazīšanas un citu mākslīgā intelekta novērošanas sistēmu pamatā ir personas datu apstrāde, datu subjektiem ir jāgarantē visas iepriekš uzskaitītās tiesības. Īpaša nozīme ir tiesībām uz informāciju, kas ir pārredzamības principa pamatā, un tiesībām nebūt automatizētu lēmumu subjektam. Būtiska nozīme mākslīgā intelekta tehnoloģiju izmantošanā ir arī pārējām tiesībām – piekļuves tiesībām, tiesībām iebilst, labot un dzēst datus, kā arī tiesībām uz efektīvu tiesību aizsardzību.

VDAR nosaka vispārīgas prasības attiecībā uz pārredzamas informācijas sniegšanu, saziņu un datu subjekta tiesību īstenošanas kārtību (VDAR 39. apsvērums, 12. pants, Policijas direktīvas 12. pants). Informācija ir jāsniedz kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu. Tā ir jāsniedz rakstiski, vajadzības gadījumā – elektroniskā formā, kā arī pēc datu subjekta pieprasījuma, un, ja ir pierādīta datu subjekta identitāte, to var sniegt arī mutiski (VDAR 12. panta 1. punkts, Policijas direktīvas 12. panta

1. punkts). Kad personas datus apstrādā, izmantojot elektroniskus līdzekļus, pārzinim ir jānodrošina arī līdzekļi, ar kuriem pieprasījumus var izdarīt elektroniski (VDAR 59. apsvērums un 12. panta 1. punkts, Policijas direktīvas 12. panta 1. punkts). Pārzinim ir jāatbild uz datu subjekta pieprasījumiem, kas saistīti ar šīs personas tiesību izmantošanu, un jāinformē par veiktajām darbībām bez nepamatotas kavēšanās (VDAR 12. panta 3. punkts, Policijas direktīvas 12. panta 3. punkts). VDAR nosaka, ka atbilde uz pieprasījumu ir jāsniedz mēneša laikā. Informācija ir jāsniedz bez maksas. Izņēmuma gadījumā, ja datu subjekta pieprasījumi ir acīmredzami nepamatoti vai pārmērīgi, it īpaši to regulāras atkārtošanās dēļ, pārzinis var vai nu pieprasīt saprātīgu maksu, vai arī atteikties izpildīt pieprasījumu. Tomēr šādā gadījumā pārzinim ir pienākums uzskatāmi parādīt, ka pieprasījums ir acīmredzami nepamatots vai pārmērīgs (VDAR 12. panta 5. punkts, Policijas direktīvas 12. panta 4. punkts). Pārzinim ir jāpārbauda datu subjekta, kas izdara pieprasījumu, identitāte, jo īpaši saistībā ar tiešsaistes pakalpojumiem un tiešsaistes identifikatoriem (VDAR 64. apsvērums, 12. panta 6. punkts, Policijas direktīvas 12. panta 5. punkts).

Datu subjektam ir tiesības piekļūt saviem datiem, lai iegūtu informāciju par apstrādi un pārliecinātos par tās likumīgumu. Piekļuves tiesības ietver tiesības saņemt apstiprinājumu par savu datu apstrādi, piekļūt attiecīgajiem datiem (t. i., iegūt to kopijas), kā arī iegūt detalizētu informāciju par apstrādi, tostarp apstrādes nolūku, personas datu kategorijām, personas datu saņēmējiem, laikposmu, cik ilgi personas dati tiks glabāti, informāciju par automatizētu lēmumu pieņemšanu u. c. (VDAR 15. panta 1. un 2. punkts, Policijas direktīvas 14. pants). Persona var pieprasīt par saviem datiem līdzīga veida informāciju, kas saskaņā ar VDAR pārzinim ir jāsniedz pirms personas datu apstrādes (VDAR 13. un 14. pants). Ja pārzinis apstrādā lielu informācijas apjomu saistībā ar datu subjektu, pārzinis var pieprasīt, lai datu subjekts jau laikus – pirms informācijas nosūtīšanas – precizē, uz kuru informāciju un kurām apstrādes darbībām pieprasījums attiecas (VDAR 15. panta 3. punkts). Pastāv neskaidrības, vai pārzinim ir jāsniedz datu subjektam tikai vispārīga informācija vai arī individuāls paskaidrojums.

Iespēja izmantot piekļuves tiesības ir daļa no tiesībām uz efektīvu tiesību aizsardzību. Lai gan datu subjekta tiesības uz piekļuvi nav tas pats, kas tiesības piekļūt lietas materiāliem, abas tiesības izriet no labas pārvaldības prasības. FRA norāda, ka tiesības uz labu pārvaldību ietver, bet neaprobežojas ar personas tiesībām piekļūt lietas materiāliem un jebkuras valsts iestādes pienākumu pamatot savus lēmumus. Piekļuve lietas materiāliem atvieglo izpratni par lēmuma pamatā esošiem pierādījumiem un iemesliem, tādējādi indivīdam dodot labākas iespējas izvirzīt pretargumentus, izmantojot tiesības tikt uzklausītam. Pienākums sniegt pamatojumu, raugoties no aizskarto personu pozīcijām, padara lēmumu pieņemšanas procesu pārredzamāku, lai attiecīgā persona varētu zināt, kāpēc ir veikts

pasākums vai darbība. Tiesības uz labu pārvaldību attiecas arī uz gadījumiem, kad tiesībaizsardzības iestādes apstrādā sejas attēlus, izmantojot sejas atpazīšanas tehnoloģijas.

Lai arī tiesības uz labu pārvaldību var būt pakļautas noteiktiem ierobežojumiem, rodas jautājums, kā nodrošināt, lai potenciāli milzīgajam personu skaitam būtu visa pieeja viņu failiem jeb glabātajiem personas datiem. Vēl viens jautājums ir, kā pārliecināties, ka policija un citas valsts iestādes vienmēr norāda iemeslus, ja kāds tiek apturēts un/vai meklēts, pamatojoties uz sejas atpazīšanas sakritību. Lai izmantotu tiesības piekļūt failiem, tostarp sistēmās saglabātajiem personas datiem, personai ir jāapzinās, ka tur tiek glabāti viņa personas dati. Cilvēki bieži nezina, ka viņu sejas attēli tiek ierakstīti un apstrādāti datubāzē salīdzināšanai. Ja viņi nezina par apstrādi, viņi arī nevar pieprasīt piekļuvi saviem datiem, kā arī izmantot citas tiesības. Tiesību uz labu pārvaldību galvenie komponenti, piemēram, tiesības piekļūt lietas materiāliem un iestādes pienākums pamatot savus lēmumus, ir skaidroti arī konkrētākos ES datu aizsardzības tiesību aktu noteikumos. Gan VDAR, gan Hartas 8. panta 2. punkts paredz, ka ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos.[597]

Datu subjektam ir arī tiesības uz savu personas datu labošanu, lai nodrošinātu, ka dati ir precīzi. Pēc datu subjekta pieprasījuma pārzinim ir pienākums bez nepamatotas kavēšanās labot neprecīzus šīs personas datus (VDAR 16. pants, Policijas direktīvas 16. panta 1. punkts). Iepriekš aplūkotais precizitātes princips uzliek pienākumu pašam pārzinim nodrošināt datu precizitāti, piemēram, regulāri lūdzot datu subjektam pārbaudīt savus personas datus. Neatbildēts paliek jautājums, kā nodrošināt to sejas attēlu precizitāti un atjaunošanu, kas izmantoti mākslīgā intelekta sistēmās. Viltus sakritības gadījumā datu subjekti var pieprasīt labojumus, lai izvairītos, ka sistēma nākotnē atkārtoti konstatē nepatiesu atbilstību.

Tiesības uz datu dzēšanu jeb tiesības "tikt aizmirstam" paredz datu subjekta tiesības panākt, lai pārzinis bez nepamatotas kavēšanās dzēstu datu subjekta personas datus, un pārziņa pienākums ir dzēst personas datus, ja vairs nepastāv personas datu likumīgas apstrādes nosacījumi (nosacījumi paredzēti VDAR 17. panta 1. punktā). Policijas direktīvas 16. panta 2. punkts nosaka, ka valstīm ir jāparedz, ka pārzinis bez nepamatotas kavēšanās dzēš personas datus un nodrošina datu subjektam tiesības panākt, lai pārzinis bez nepamatotas kavēšanās dzēstu personas datus, kas uz šo personu attiecas, ja apstrāde pārkāpj personas datu apstrādes pamatprincipus (4. pants), apstrādes likumības prasību (8. pants) vai īpašu kategoriju personas datu apstrādes nosacījumus (10. pants) vai ja personas dati ir jādzēš, lai izpildītu uz pārzini attiecināmu juridisku pienākumu.

597 FRA (2019), Facial recognition technology.

Neskaidrs ir jautājums, vai pienākums dzēst personas datus ietver arī izsecinātos personas datus vai arī izsecinātos grupas datus, piemēram, apmācīto algoritmisko modeli. Dž. Sartors uzskata, ka pirmajā gadījumā atbilde varētu būt pozitīva, bet otrajā negatīva, jo apmācītais algoritma modelis vairs nav personisks. Tajā pašā laikā, izdzēšot datus, ko izmanto algoritmiskā modeļa izveidošanai, var būt grūti vai neiespējami pierādīt šī modeļa pareizību.[598]

Policijas direktīvas 16. panta 3. punkts paredz, ka dzēšanas vietā pārzinis ierobežo apstrādi, ja

1) datu subjekts apstrīd personas datu precizitāti un to precizitāti vai neprecizitāti nevar noteikt;
2) personas dati ir jāsaglabā pierādījumu nolūkā.

Otrajā gadījumā pārzinis informē datu subjektu pirms apstrādes ierobežojuma atcelšanas.

Arī VDAR 18. panta 1. punkts nosaka, ka datu subjektam ir tiesības panākt, lai pārzinis ierobežotu apstrādi, ja ir viens no šādiem apstākļiem:

a) datu subjekts apstrīd personas datu precizitāti – uz laiku, kurā pārzinis var pārbaudīt personas datu precizitāti;
b) apstrāde ir nelikumīga, un datu subjekts iebilst pret personas datu dzēšanu un tās vietā pieprasa datu izmantošanas ierobežošanu;
c) pārzinim personas dati apstrādei vairs nav vajadzīgi, taču tie ir nepieciešami datu subjektam, lai celtu, īstenotu vai aizstāvētu likumīgas prasības;
d) datu subjekts ir iebildis pret apstrādi, līdz nav pārbaudīts, vai pārziņa leģitīmie iemesli nav svarīgāki par datu subjekta leģitīmajiem iemesliem.

Ja apstrāde ir ierobežota, personas datus ir atļauts tikai glabāt, bet apstrādāt tos citādā veidā var tikai ar datu subjekta piekrišanu vai tādēļ, lai celtu, īstenotu vai aizstāvētu likumīgas prasības, vai lai aizsargātu citas fiziskas vai juridiskas personas tiesības, vai ES vai dalībvalstu svarīgu sabiedrības interešu dēļ (VDAR 18. panta 2. punkts).

Policijas direktīva paredz datu subjektu tiesību ierobežojumus – piekļuves tiesību (15. pants), tiesību uz informāciju (13. panta 3. punkts), tiesību labot un dzēst datus un ierobežot datu apstrādi (16. panta 4. punkts) –, kas izriet no tiesībaizsardzības iestāžu pienākuma strādāt noteiktā konfidencialitātes un slepenības pakāpē un nodrošināt to darba efektivitāti. Ja datu apstrādes mērķis ir noziedzīgu nodarījumu novēršana, izmeklēšana, atklāšana vai kriminālvajāšana, kriminālsodu izpilde vai sabiedrības drošības nodrošināšana, minētās tiesības var tikt ierobežotas, ja tas nepieciešams, lai:

a) novērstu, ka tiek traucētas oficiālas vai juridiskas pārbaudes, izmeklēšanas vai procedūras;

598 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

b) novērstu, ka tiek kaitēts noziedzīgu nodarījumu novēršanai, atklāšanai, izmeklēšanai vai saukšanai pie atbildības par tiem, vai kriminālsodu izpildei;
c) aizsargātu sabiedrisko drošību;
d) aizsargātu valsts drošību;
e) aizsargātu citu personu tiesības un brīvības (Policijas direktīvas 13. panta 3. punkts, 15. panta 1. punkts, 16. panta 4. punkts).

Šiem ierobežojumiem ir jābūt noteiktiem tiesību aktos un ir jābūt nepieciešamiem un samērīgiem demokrātiskā sabiedrībā. Nacionālajā regulējumā ir jānosaka pārziņa pienākums bez nepamatotas kavēšanās rakstiski informēt datu subjektu par atteikumu vai ierobežojumu piekļūt datiem un par atteikuma vai ierobežojuma iemesliem, izņemot, ja tas apdraud kādu no minētajiem mērķiem. Pārzinim ir jāinformē datu subjekts arī par iespēju iesniegt sūdzību uzraudzības iestādei vai vērsties tiesā (Policijas direktīvas 15. panta 3. punkts). Pārzinim ir jādokumentē faktiskie vai juridiskie iemesli, kuri ir lēmuma pamatā, un šī informācija jādara pieejama uzraudzības iestādēm (Policijas direktīvas 15. panta 4. punkts). Pārzinim ir rakstiski jāinformē datu subjekts par atteikumu labot personas datus, tos dzēst vai ierobežot apstrādi un par atteikuma iemesliem.

VDAR ir noteiktas vēl vairākas tiesības, kas nav paredzētas Policijas direktīvā, ņemot vērā tās darbības jomu, kas saistīta ar noziedzīgu nodarījumu novēršanu un atklāšanu. VDAR ievieš jaunas tiesības uz datu pārnesamību. To mērķis ir paplašināt datu subjektu iespējas attiecībā uz viņu personas datiem, veicinot viņu spēju viegli pārvietot, kopēt un nosūtīt personas datus no vienas informācijas tehnoloģiju vides uz citu. Tiesības uz datu pārnesamību garantē datu subjektam tiesības saņemt personas datus attiecībā uz sevi, kurus viņš sniedzis pārzinim, strukturētā, plaši izmantotā un mašīnlasāmā formātā un nosūtīt tos citam pārzinim (VDAR 20. panta 1. punkts). Tiesības uz datu pārnesamību ir piemērojamas tikai gadījumā, ja apstrāde tiek veikta ar automatizētiem līdzekļiem. Pārzinim šīs tiesības ir jānodrošina tikai tad, ja personas datu apstrāde ir veikta uz piekrišanas pamata vai tā ir nepieciešama, lai izpildītu līgumu, savukārt tās nav piemērojamas, ja apstrāde tiek veikta, pamatojoties uz citu tiesisko pamatu.

VDAR paredz datu subjektam, balstoties uz iemesliem saistībā ar viņa īpašo situāciju, tiesības jebkurā laikā iebilst pret savu personas datu apstrādi, ja apstrādes tiesiskais pamats ir:

- uzdevumu izpilde, ko veic sabiedrības interesēs vai īstenojot pārzinim piešķirtās oficiālās pilnvaras, vai
- pārziņa vai trešās personas leģitīmo interešu ievērošana (21. panta 1. punkts).

Ja datu subjekts iebilst pret šādu apstrādi, pārzinim ir jāpārvērtē leģitīmo interešu samērīgums ar datu subjekta interesēm (VDAR 21. panta 1. punkts).

Pārzinim ir jāpārtrauc personas datu apstrāde, izņemot, ja tas var norādīt uz pārliecinošiem apstrādes iemesliem, kas ir svarīgāki par datu subjekta pamattiesībām un brīvībām (VDAR 69. apsvērums, 21. panta 1. punkts). Datu subjektam ir tiesības iebilst pret savu personas datu apstrādi tiešās tirgvedības nolūkos, tostarp iebilst pret profilēšanu, ciktāl tā saistīta ar šādu tiešo tirgvedību, gan uzsākot datu apstrādi, gan tās laikā (VDAR 21. panta 2. punkts). Gadījumā, kad persona ir piekritusi datu apstrādei, viņa var izmantot tiesības atsaukt savu piekrišanu jebkurā laikā (VDAR 7. panta 3. punkts), tāpēc tiesības iebilst nav attiecināmas uz apstrādi, kas veikta uz piekrišanas pamata. Ja datu subjekts iebilst pret datu apstrādi tiešās tirgvedības nolūkā, pārzinis personas datus šādam nolūkam vairs nedrīkst apstrādāt (VDAR 21. panta 3. punkts).

Arī VDAR paredz izņēmumus attiecībā uz datu subjekta tiesību ierobežošanu, kā arī datu apstrādes principu ierobežošanu. Saskaņā ar ES un dalībvalstu leģislatīviem pasākumiem, kas piemērojami datu pārzinim un apstrādātājam, var ierobežot pienākumu un tiesību darbības jomu attiecībā uz personas datu apstrādes principiem, datu subjekta tiesībām, kā arī attiecībā uz pārziņa pienākumu ziņot datu subjektam par personas datu aizsardzības pārkāpumiem (VDAR 23. panta 1. punkts). Šādi ierobežojumi ir pieļaujami, ciktāl "tiek ievērota pamattiesību un pamatbrīvību būtība un tas demokrātiskā sabiedrībā ir nepieciešams un samērīgs", lai garantētu būtiskus sabiedrības interešu mērķus: valsts drošību; aizsardzību; sabiedrisko drošību; noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu vai saukšanu pie atbildības par tiem vai kriminālsodu izpildi, tostarp aizsardzību pret sabiedriskās drošības apdraudējumiem un to novēršanu; citus svarīgus ES vai dalībvalsts vispārējo sabiedrības interešu mērķus, datu subjekta aizsardzību vai citu personu tiesību un brīvību aizsardzību u. c. (VDAR 23. panta 1. punkts).

Paredzot šādus ierobežojumus, tiesību aktā ir jāietver arī konkrēti noteikumi vismaz par

- nolūkiem, kādos veic apstrādi, vai par apstrādes kategorijām;
- personas datu kategorijām;
- ieviesto ierobežojumu darbības jomu;
- garantijām, lai novērstu datu ļaunprātīgu izmantošanu vai nelikumīgu piekļuvi vai nosūtīšanu;
- pārziņa vai pārziņu kategoriju noteikšanu;
- glabāšanas laikposmiem un piemērojamām garantijām, ņemot vērā apstrādes vai apstrādes kategoriju raksturu, darbības jomu un nolūku;
- riskiem attiecībā uz datu subjektu tiesībām un brīvībām;
- datu subjektu tiesībām saņemt informāciju par ierobežojumu, izņemot tad, ja tas var kaitēt ierobežojuma mērķim (VDAR 23. panta 2. punkts).

Konvencija 108+ pieļauj izņēmumus no personas datu apstrādes pamatprincipiem un datu subjekta tiesībām, ja šādi izņēmumi ir paredzēti likumā, respektē

pamattiesību un brīvību būtību un ir nepieciešami un samērīgi pasākumi demokrātiskā sabiedrībā, lai

- aizsargātu valsts drošības, aizsardzības, sabiedrības drošības, svarīgas valsts ekonomiskās un finansiālās intereses, tiesu varas objektivitāti un neatkarību vai noziedzīgu nodarījumu novēršanu, izmeklēšanu un kriminālvajāšanu, kā arī kriminālsodu izpildi un citas būtiskas vispārējās sabiedrības intereses;
- aizsargātu datu subjekta vai citu personu tiesības un pamatbrīvības, īpaši vārda brīvību (11. panta 1. punkts).

Tiesību aktā var paredzēt izņēmumus no pārredzamības un informēšanas prasībām, ja dati tiek apstrādāti arhivēšanas nolūkos sabiedrības interesēs, zinātnisko vai vēsturisko pētījumu vai statistikas vajadzībām, ja nepastāv risks, ka tiks pārkāptas datu subjektu tiesības un pamatbrīvības (11. panta 2. punkts). Konvencija 108+ turklāt nosaka, ka, atsaucoties uz apstrādes darbībām valsts drošības un aizsardzības nolūkos, valsts ar likumu var paredzēt izņēmumus arī no citām prasībām, piemēram, kas attiecas uz pārrobežu datu nodošanu, uzraudzības iestāžu pienākumiem un valsts pienākuma atļaut Konvencijas komitejai izvērtēt pasākumu efektivitāti, ciktāl tas ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā, lai sasniegtu šo mērķi. Tas neskar prasību, ka apstrādes darbības valsts drošības un aizsardzības nolūkos tiek pakļautas neatkarīgai un efektīvai pārskatīšanai un uzraudzībai saskaņā ar attiecīgās valsts nacionālajiem tiesību aktiem (11. panta 3. punkts). VDAR, Policijas direktīva un Konvencija 108+ paredz iespējas valstij noteikt daudzus izņēmumus no datu aizsardzības noteikumiem.

Lai nodrošinātu apstrādes likumību un lai izvairītos no patvaļīgas datu apstrādes un iespējamiem pārkāpumiem, īpaša nozīme ir efektīvas uzraudzības un tiesību aizsardzības nodrošināšanai. Tiesību ierobežošanas gadījumā tiesībaizsardzības iestādēm ir jāinformē personas, cita starpā, par piemērotajiem pasākumiem, ja šis paziņojums vairs nespēj apdraudēt šo iestāžu veiktās izmeklēšanas, kā arī par tiesībām iesniegt sūdzību uzraudzības iestādēm un tiesībām uz efektīvu tiesību aizsardzību. Šis pienākums attiecas arī uz datiem, kas tiek apstrādāti, izmantojot sejas atpazīšanas un citas novērošanas tehnoloģijas. Cilvēki var vēlēties apstrīdēt sejas attēla iekļaušanu "novērošanas sarakstā", iebilstot, ka tas darīts nepārredzamā veidā un bez viņu piekrišanas, vai var pieprasīt atlīdzību par viltus pozitīvas atbilstības konstatēšanu, kas viņiem radījusi negatīvas sekas (piemēram, nelikumīga aizturēšana, meklēšana vai arests), tai skaitā pieprasīt atlīdzību par visiem nodarītajiem zaudējumiem (piemēram, ja persona nokavējusi savienoto lidojumu vai viņai nepamatoti liegta iebraukšana ES valstī).[599] Turklāt iespēja vienīgi iesniegt administratīvu sūdzību uzraudzības iestādē netiek

599 FRA (2019), Facial recognition technology.

uzskatīta par efektīvu tiesību aizsardzības līdzekli, piemēram, saskaņā ar Hartas 47. pantu, jo tiesa netiek iesaistīta šādā pārskatīšanā. Ja iekšējie un alternatīvie strīdu izšķiršanas mehānismi izrādās nepietiekami vai ja attiecīgā persona vēlas, lai lieta tiktu pārskatīta tiesā, vienmēr ir jābūt iespējai lietu apstrīdēt tiesā.[600] Lai nodrošinātu iestāžu veiktās apstrādes likumību un novērstu patvaļīgu un pretiesisku datu apstrādi, būtiska nozīme ir atbildības mehānismiem un neatkarīgu iestāžu veiktai šo mehānismu pārraudzībai, no kuriem viens no būtiskākajiem ir ietekmes novērtējums.

6.5. Novērtējums par ietekmi uz datu aizsardzību

Viens no nozīmīgākajiem atbildības mehānismiem, kas ir noteikts ES datu aizsardzības tiesību aktos, ir novērtējums par ietekmi uz datu aizsardzību. Tas ļauj novērtēt apstrādes darbības, to iespējamos riskus attiecībā uz personu tiesībām un brīvībām, kā arī noteikt pasākumus šo risku mazināšanai un novēršanai.

VDAR nosaka, ka novērtējums ir obligāti jāveic, ja plānotās apstrādes darbības varētu radīt augstu risku fizisku personu tiesībām un brīvībām (35. panta 1. punkts). VDAR 35. panta 3. punkts nosaka kritērijus, kad novērtējums ir īpaši vajadzīgs. Tie ir:

1) ar fiziskām personām saistītu personisku aspektu sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde, tostarp profilēšana, un ar kuru pamato lēmumus, kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu;
2) īpašo kategoriju datu vai personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā;
3) publiski pieejamas zonas sistemātiska uzraudzība plašā mērogā.

Līdzās minētajiem gadījumiem apstrāde var radīt augstu risku arī citos gadījumos, un pārzinim var būt pienākums veikt novērtējumu. 29. panta darba grupa ir noteikusi deviņus kritērijus, kas jāņem vērā pārziņiem, novērtējot, vai apstrādes darbības "varētu radīt augstu risku" un attiecīgi vai ir veicams novērtējums. Šie kritēriji ir:

1) vērtēšana vai punktu piešķiršana, tostarp profilēšana un prognozes;
2) automatizēti lēmumi, kuriem ir tiesiskas vai līdzīgi būtiskas sekas;
3) sistemātiska novērošana;
4) sensitīvi vai ļoti personiska rakstura dati;
5) datu apstrāde plašā mērogā;
6) datu kopu saskaņošana vai apkopošana;

600 FRA (2019), Facial recognition technology.

7) dati par neaizsargātiem datu subjektiem;
8) jaunu tehnoloģisko vai organizatorisko risinājumu izmantošana vai piemērošana;
9) ja apstrāde kavē datu subjektus īstenot savas tiesības vai izmantot pakalpojumu vai līgumu.

Vairākumā gadījumu datu pārzinis var uzskatīt, ka tad, ja apstrāde atbilst diviem kritērijiem, attiecībā uz to ir jāveic novērtējums, un, jo vairāk kritērijiem apstrāde atbilst, jo lielāka ir varbūtība, ka tā radīs augstu risku datu subjektu tiesībām un brīvībām.[601] Uzraudzības iestādēm ir jāizstrādā un jāpublisko saraksts ar tām apstrādes darbībām, kurām ir jāveic novērtējums, un tās arī var izstrādāt sarakstu ar apstrādes darbībām, kam novērtējums nav jāveic (VDAR 35. panta 4. un 5. punkts).[602]

VDAR turklāt paredz, ka valsts tiesību aktos var būt noteikts, ka pārzinim ir jāapspriežas ar uzraudzības iestādi un jāsaņem no tās iepriekšēja atļauja saistībā ar apstrādi, ko tas veic, lai izpildītu sabiedrības interesēs īstenojamu uzdevumu, tostarp, kad minēto apstrādi veic saistībā ar sociālo aizsardzību un sabiedrības veselību (36. panta 5. punkts).

Pārzinis var izmantot dažādas metodoloģijas novērtējuma veikšanai. ES dalībvalstu uzraudzības iestādes ir publicējušas dažādas vadlīnijas, kā arī tiešsaistes rīkus[603], lai palīdzētu uzņēmumiem un organizācijām sagatavot novērtējumus. VDAR 35. panta 7. punkts nosaka, ka novērtējumā ietver vismaz

a) plānoto apstrādes darbību un apstrādes nolūku, tostarp attiecīgā gadījumā pārziņa leģitīmo interešu sistemātisku aprakstu;
b) novērtējumu par apstrādes darbību nepieciešamību un samērīgumu attiecībā uz nolūkiem;
c) novērtējumu par riskiem datu subjektu tiesībām un brīvībām;
d) pasākumus, kas paredzēti risku novēršanai, tostarp garantijas, drošības pasākumus un mehānismus, ar ko nodrošina personas datu aizsardzību

601 Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/611236/en

602 Sk. Datu valsts inspekcija. (2018). Apstrādes darbību veidi, attiecībā uz kuriem ir jāveic datu aizsardzības ietekmes novērtējums saskaņā ar VDAR 35. panta 4. punktu. https://www.dvi.gov.lv/lv/media/92/download

603 Sk., piemēram, ICO. Data Protection Impact Assessments (DPIAs). https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/; CNIL. (2019). The open source PIA softwere helps to carry out data protection impact assessment. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

un uzskatāmi parāda, ka ir ievērota VDAR, ņemot vērā datu subjektu un citu attiecīgo personu tiesības un leģitīmās intereses.

Pārzinim ir jālūdz padoms datu aizsardzības speciālistam, ja tāds ir iecelts (VDAR 35. panta 2. punkts), piemēram, par šādiem jautājumiem: ir vai nav jāveic novērtējums; kāda metodika ir jāizmanto; kādi drošības pasākumi ir jāveic, lai mazinātu datu subjektu tiesību un interešu risku; vai novērtējums ir veikts pareizi; vai secinājumi atbilst VDAR u. c.[604]

Policijas direktīva arī nosaka pienākumu veikt novērtējumu par ietekmi uz datu aizsardzību. Ja apstrādes veids, jo īpaši izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus, varētu radīt augstu risku fizisko personu tiesībām un brīvībām, valsts paredz, ka pārzinis pirms apstrādes veic novērtējumu par to, kā plānotās apstrādes darbības ietekmēs personas datu aizsardzību (27. panta 1. punkts). Šajā novērtējumā ietver vismaz plānoto apstrādes darbību vispārīgu aprakstu, novērtējumu par riskiem datu subjektu tiesībām un brīvībām, pasākumus, kas paredzēti minēto risku novēršanai, garantijas, drošības pasākumus un mehānismus, ar kuriem nodrošina personas datu aizsardzību un uzskatāmi parāda, ka ir ievērota Policijas direktīva, ņemot vērā datu subjektu un citu attiecīgo personu tiesības un leģitīmās intereses (27. panta 2. punkts).

Gan VDAR, gan Policijas direktīva paredz iepriekšēju apspriešanos ar uzraudzības iestādi. VDAR nosaka – ja novērtējumā tiek konstatēts, ka gadījumā, ja pārzinis neveiktu pasākumus riska mazināšanai, apstrāde radītu augstu risku, pārzinim pirms apstrādes ir jāapspriežas ar uzraudzības iestādi (36. panta 1. punkts). Ja uzraudzības iestāde uzskata, ka plānotā apstrāde pārkāptu VDAR, it īpaši tad, ja pārzinis nav pietiekami identificējis vai mazinājis risku, tā sniedz pārzinim un attiecīgā gadījumā apstrādātajam rakstisku padomu un var izmantot citas izmeklēšanas pilnvaras (36. panta 2. punkts). Apspriežoties ar uzraudzības iestādi, pārzinis sniedz tai nepieciešamo informāciju par apstrādi, tās nolūkiem, līdzekļiem, pasākumiem un garantijām, lai nodrošinātu datu subjektu tiesību un brīvību aizsardzību saskaņā ar VDAR (36. panta 3. punkts).

Policijas direktīva savukārt nosaka, ka valsts paredz pienākumu pārzinim vai apstrādātājam apspriesties ar uzraudzības iestādi pirms tādu personas datu apstrādes, ko ietvers jaunizveidotā kartotēkā, ja

1) novērtējumā par ietekmi uz datu aizsardzību ir norādīts, ka gadījumā, ja pārzinis neveiktu pasākumus riska mazināšanai, apstrāde radītu augstu risku; vai

604 Article 29 Data Protection Working Party (2016), Guidelines on Data Protection Officers ('DPOs').

2) apstrādes veids, jo īpaši tāds, kurā izmantotas jaunas tehnoloģijas, mehānismi vai procedūras, ir saistīts ar augstu risku datu subjektu tiesībām un brīvībām (28. panta 1. punkts).

Pārzinim ir jāiesniedz uzraudzības iestādei novērtējums par ietekmi uz datu aizsardzību un pēc pieprasījuma jebkura cita informācija, kas ļauj tai izvērtēt apstrādes atbilstību, jo īpaši riskus datu subjekta personas datu aizsardzībai un attiecīgās garantijas (28. panta 4. punkts).

Lai gan Konvencija 108+ neparedz ietekmes novērtējumu kā atsevišķu atbildības mehānismu, tajā ir noteikts, ka valsts nodrošina, ka pārziņi un attiecīgā gadījumā apstrādātāji pirms datu apstrādes uzsākšanas pārbauda paredzētās datu apstrādes iespējamo ietekmi uz datu subjektu tiesībām un pamatbrīvībām un plāno datu apstrādi tā, lai novērstu vai samazinātu risku iejaukties šajās tiesībās un pamatbrīvībās (10. panta 2. punkts).

Sejas atpazīšanas tehnoloģiju izmantošanas gadījumā pārzinim ir jāveic novērtējums par ietekmi uz datu aizsardzību.[605] VDAR 35. pantā un Policijas direktīvas 28. pantā noteiktie kritēriji, kas ļauj izvērtēt, vai ir jāveic novērtējums, īpaši saistībā ar jauno tehnoloģiju izmantošanu, lielā mērā ir attiecināmi uz sejas atpazīšanas tehnoloģiju izmantošanu. Datu valsts inspekcijas publicētajā sarakstā ar tām apstrādes darbībām, attiecībā uz kurām ir jāveic novērtējums, ir ietverta arī "inovatīva jaunu tehnoloģiju vai risinājumu izmantošana vai to pielietošana, piemēram, apvienojot pirkstu nospiedumu un sejas atpazīšanas lietošanu, lai uzlabotu piekļuves kontroli utt."[606] VDAR turklāt paredz, ka novērtējums ir īpaši vajadzīgs, apstrādājot īpašu kategoriju personas datus vai personas datus par sodāmību un pārkāpumiem plašā mērogā (35. panta 3. punkta b) apakšpunkts), kā arī veicot publiski pieejamu zonu uzraudzību plašā mērogā (35. panta 3. punkta c) apakšpunkts). Sejas atpazīšanas tehnoloģijas ietver biometrisko datu apstrādi, un to izmantošanas nolūks var būt saistīts ar publiskas telpas uzraudzību plašā mērogā. Novērtējuma veikšana pirms apstrādes uzsākšanas ļauj noteikt, vai konkrētajā gadījumā sejas atpazīšanas tehnoloģijas izmantošana ir pieļaujama.

Pirms jaunu tehnoloģiju ieviešanas, ja to veiktā personas datu apstrāde var aizskart personu pamattiesības, ir jāiesaista uzraudzības iestāde. Gan VDAR, gan Policijas direktīva paredz, ka valsts apspriežas ar uzraudzības iestādi, kamēr tiek gatavots priekšlikums leģislatīvam pasākumam, ko pieņems valsts parlaments, vai regulatīvs pasākums, kas balstās uz šādu leģislatīvu pasākumu, kurš attiecas uz apstrādi (VDAR 36. panta 4. punkts, Policijas direktīvas 28. panta 2. punkts). Turklāt datu aizsardzības novērtējums atsevišķos gadījumos var nebūt pietiekams, jo līdzās riskiem datu subjekta tiesībām un brīvībām var būt jāvērtē to plašāka

605 EDPB (2019), Guidelines 3/2019 on processing of personal data through video devices.

606 Sk. Datu valsts inspekcija (2018), Apstrādes darbību veidi, attiecībā uz kuriem ..

ietekme uz sabiedrību un demokrātiju. Lai gan Latvijā sejas atpazīšanas tehnoloģijas sabiedriskās vietās nav ieviestas, Iekšlietu ministrija ir apsvērusi iespēju izveidot vienotu videonovērošanas kameru tīklu ar sejas atpazīšanas programmatūru.[607] Pirms jaunu novērošanas tehnoloģiju ieviešanas ir būtiski noskaidrot gan Datu valsts inspekcijas, gan citu tiesībaizsardzības iestāžu, piemēram, Tiesībsarga biroja, viedokli. Tāpat svarīgi ir uzzināt personu, kuru dati tiks apstrādāti, viedokli. VDAR paredz, ka attiecīgā gadījumā pārzinim ir jāprasa datu subjektu vai viņu pārstāvju viedoklis par plānoto apstrādi, izvērtējot šādu iepriekšēju konsultēšanās nepieciešamību katrā konkrētajā gadījumā (35. panta 9. punkts). Policijas direktīva šādu prasību neparedz. Tajā pašā laikā tādu tehnoloģiju ieviešana, kas būtiski ierobežo cilvēktiesības, nedrīkstētu notikt bez sabiedrības viedokļa uzklausīšanas un tās atbalsta.

Nākamā grāmatas nodaļa veltīta ieteikumiem, kā attīstīt mākslīgā intelekta novērošanas tehnoloģiju regulējumu, atbildības un uzraudzības mehānismus. Bet vispirms sniegts ieskats, kā datu aizsardzības standarti tika attiecināti uz kontakta izsekošanas lietotnēm, kas bija viena no tehnoloģijām, kuru ieviesa cīņā ar koronavīrusa pandēmiju. Tās izvērtējums var palīdzēt attīstīt uzraudzības mehānismus un regulējumu arī attiecībā uz citām tehnoloģijām, tostarp mākslīgā intelekta novērošanas tehnoloģijām.

6.6. Datu aizsardzības standarti kontaktu izsekošanas lietotnēm

Lai novērstu sabiedrības bažas par personas datu prettiesisku izmantošanu un atbalstītu valstis un lietotņu izstrādātājus, daudzas starptautiskas, ES un valstu iestādes izstrādāja vadlīnijas, kas skaidro datu aizsardzības prasības kontaktu izsekošanas lietotnēm. 2020. gada 16. aprīlī Eiropas Komisija publicēja divas pamatnostādnes, lai atbalstītu vienotu koordinētu pieeju kontaktu izsekošanas lietotņu izmantošanai visās ES valstīs. ES dalībvalstu e-veselības tīkls ar Eiropas Komisijas atbalstu izstrādāja ES rīkkopu mobilo lietojumprogrammu izmantošanai kontaktu izsekošanai un brīdināšanai.[608] Kopā ar rīkkopu Eiropas Komisija pieņēma Norādījumus par lietotnēm, kas sniedz atbalstu cīņā pret Covid-19

607 Spundiņa, L. (1. oktobris 2020). Datu valsts inspekcija neatbalsta sejas atpazīšanas videonovērošanas iekārtas. *LSM.lv*. https://www.lsm.lv/raksts/zinas/latvija/datu-valsts-inspekcija-neatbalsta-sejas-atpazisanas-videonoverosanas-iekartas.a376399/

608 E-health Network. (2020). Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States. https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19_apps_en.pdf

pandēmiju saistībā ar datu aizsardzību.[609] 2020. gada 21. aprīlī Eiropas Datu aizsardzības kolēģija pieņēma pamatnostādnes par atrašanās vietas datu un kontaktu izsekošanas rīku izmantošanu saistībā ar Covid-19 uzliesmojumu.[610] Šajos dokumentos ir noteikti datu aizsardzības standarti kontaktu izsekošanas lietotnēm, lai tās atbilstu ES datu aizsardzības regulējumam.

Arī citas starptautiskas organizācijas pieņēma vairākas vadlīnijas. 2020. gada 21. aprīlī Eiropas Padome publicēja kopīgu paziņojumu par digitālo kontaktu izsekošanu.[611] OECD 2020. gada 23. aprīlī publicēja dokumentu par Covid-19 izsekošanu un privātuma un datu aizsardzību, izmantojot lietotnes un biometriskos datus.[612]

Šie dokumenti nosaka kopīgas minimālās datu aizsardzības prasības kontaktu izsekošanas lietotnēm. FRA veiktajā pētījumā ir norādīts, ka visos vai lielākajā daļā no iepriekš minētajiem dokumentiem ir noteiktas šādas prasības:

1) pierādīta efektivitāte pirms izstrādes;
2) brīvprātīgums;
3) iepriekšējs ietekmes novērtējums;
4) integrēta datu aizsardzība;
5) noteikts mērķis un juridiskais pamats;
6) atvērtais pirmkods un pārredzamība;
7) datu minimizēšana un precizitāte;
8) kontaktu noteikšanas tehniskā precizitāte;
9) anonīmi un pseidonimizēti dati;
10) drošība pret kiberuzbrukumiem;
11) atrašanās vietas datu neapstrādāšana;
12) regulāra neatkarīga uzraudzība;
13) savstarpējā savietojamība;

609 Eiropas Komisija. (2020). Komisijas paziņojums. Norādījumi par lietotnēm, kas sniedz atbalstu cīņā pret Covid-19 pandēmiju saistībā ar datu aizsardzību. *OV C* 124/1, 17.04.2020. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020XC0417(08)&from=EN

610 Eiropas Datu aizsardzības kolēģija. (2020). Pamatnostādnes 04/2020 par atrašanās vietas datu un kontaktu izsekošanas rīku izmantošanu saistībā ar Covid-19 uzliesmojumu. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_lv.pdf

611 Council of Europe. (2020). Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7

612 OECD. (2020). Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics. https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics/

14) deaktivizēšana un dzēšana pēc pandēmijas;
15) dalībnieku atbildība.[613]

Teorētiski kontaktu izsekošanas lietotnēm būtu jāatbilst visām šīm datu aizsardzības prasībām. Tomēr, lai gan valstu starpā pastāvēja vienprātība par daļu no prasībām, piemēram, brīvprātīgumu un īslaicīgumu, dažas prasības netika ievērotas vai tika izmantotas atšķirīgas pieejas. Piemēram, kas attiecas uz prasību pēc tiesību aktiem, dažas ES valstis izstrādāja speciālus tiesību aktus kontaktu izsekošanas lietotnēm, lai nodrošinātu juridisko pamatu un precizētu personu datu apstrādi, kā arī lai valsts iestādes varētu ieviest un izmantot lietotnes. Tomēr daudzās valstīs šāda likumdošana netika izstrādāta, un dažas valstis arī noliedza tās nepieciešamību.[614]

Lai nodrošinātu atbilstību datu aizsardzības regulējumam, viena no prasībām ir veikt kontaktu izsekošanas lietotnes ietekmes uz datu aizsardzību novērtējumu un to publiskot. Eiropas Datu aizsardzības kolēģija norāda, ka ir jāveic novērtējums pirms šo lietotņu ieviešanas, jo tās ietver veselības datu plašu apstrādi, sistemātisku uzraudzību un jaunu tehnoloģisku risinājumu izmantošanu, kas var radīt augstu risku personu tiesībām un brīvībām.[615] Būtiska prasība ir arī datu aizsardzības iestāžu iepriekšēja un pastāvīga iesaistīšanās kontaktu izsekošanas lietotņu izstrādē un novērtēšanā. Lai gan vairākums ES valstu, to skaitā Latvija pirms lietotnes "Apturi Covid" ieviešanas, konsultējās ar datu aizsardzības iestādēm par lietotņu izmantošanu, daudzas valstis iepriekš neveica ietekmes uz datu aizsardzību novērtējumu. Iepriekšēja novērtējuma trūkums rada bažas par pārredzamības, pārskatatbildības, datu aizsardzības un privātuma prasību ievērošanu.[616]

Dažas ES un starptautisko organizāciju ieteiktās prasības var pārsniegt datu aizsardzības regulējuma prasības, piemēram, prasība pēc atvērtā pirmkoda un publiski pieejama ietekmes novērtējuma, bet tās palīdz nodrošināt pārredzamību.[617] Augsts pārredzamības līmenis ir būtisks kontaktu izsekošanas lietotņu akceptēšanai sabiedrībai, sabiedrības kontrolei un uzticības veicināšanai.

Jebkuras kontaktu izsekošanas lietotnes efektivitāte ir atkarīga no plaša sabiedrības atbalsta. Viena no galvenajām problēmām ir nodrošināt, ka lietotnes izmanto plaša sabiedrības daļa. Sabiedrības atbalstu var veicināt, izvēloties datu minimizēšanas prasībām atbilstošāko risinājumu.

613 FRA (2020), Coronavirus pandemic in the EU ..

614 Ibid.

615 Eiropas Datu aizsardzības kolēģija (2020), Pamatnostādnes 04/2020 ..

616 FRA (2020), Coronavirus pandemic in the EU ..

617 Eiropas Datu aizsardzības kolēģija (2020), Pamatnostādnes 04/2020 ..

Jaunās pieejas datu vākšanai un apstrādei kontaktu izsekošanas lietotnēs radīja plašas diskusijas. Atbilstoši vadlīnijās sniegtajiem ieteikumiem lielākajā daļā ES valstu, ieskaitot Latviju, kontaktu izsekošanas lietotnes darbojās, izmantojot *Bluetooth* tehnoloģiju, kas ļauj konstatēt savienojumu starp ierīcēm, tomēr dažās valstīs tika izmantoti arī atrašanās vietas dati. Piemēram, Norvēģija apturēja savu kontaktu izsekošanas lietotni pēc tam, kad datu aizsardzības iestāde paziņoja, ka tā rada nesamērīgus draudus lietotāju privātumam, tostarp izmantojot atrašanās vietas datus.[618]

Kontaktu izsekošanas lietotnes var balstīt uz centralizētu vai decentralizētu pieeju. Lielākā daļa ES valstu, arī Latvija, izvēlējās decentralizētu pieeju, kur lietotāju dati tiek saglabāti viņu ierīcēs, tomēr dažās valstīs, piemēram, Francijā, tika ieviestas lietotnes ar centralizētu pieeju, kur lietotāju dati tiek glabāti un apstrādāti centrālajā serverī.[619] Lai gan Eiropas Komisija un Eiropas Datu aizsardzības kolēģija nav devusi priekšroku nevienai no abām pieejām, tiek uzskatīts, ka decentralizētais risinājums vairāk atbilst datu minimizēšanas principam.

Lielākā daļa ES dalībvalstu, izstrādājot nacionālās kontaktu izsekošanas lietotnes, izmantoja publiski pieejamus protokolus. Pirmā tika piedāvāta Viseiropas privātuma saglabāšanas tuvuma izsekošanas (PEPP-PT) iniciatīva, kas paredzēja centralizētu mehānismu, tai sekoja decentralizēta alternatīva (DP-3T). Pēc tam "Apple" un "Google" paziņoja, ka izstrādās lietojumprogrammu saskarni (*Exposure Notification API* – angļu val.), pamatojoties uz decentralizētu pieeju, kā arī norādīja, ka tā neatbalstīs centralizētu lietotņu arhitektūru. Kaut arī daudzas valstis sākotnēji izvēlējās centralizētu pieeju, pēc "Apple" un "Google" paziņojuma vairākas valstis, tostarp Lielbritānija, Itālija un Vācija, atteicās no centralizētas lietotnes ieviešanas un nolēma atbalstīt šo decentralizēto pieeju. Daudzas citas Eiropas valstis, ieskaitot Latviju, Igauniju, Somiju, Austriju, Īriju, Čehiju un Šveici, arī ieviesa lietotnes, kuru pamatā ir "Apple" un "Google" decentralizētais modelis.[620] Turklāt "Apple" operētājsistēmas iOS 13.7 atjauninājumā ieviesa funkciju *Exposure Notification Express,* kas ļauj *iPhone* lietotājiem veikt kontaktu izsekošanu bez nepieciešamības lejupielādēt oficiālu Covid-19 lietotni.[621] Iepriekš

618 Manancourt (15 June, 2020), Norway suspends contact-tracing app over privacy concerns.

619 European Commission. (2020). Mobile applications to support contact tracing in the EU's fight against COVID-19. Progress reporting June 2020. https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf

620 Sk. Rahman, M. (25 February, 2021). Here are the countries using Google and Apple's COVID-19 Contact Tracing API. *XDA Developers.* https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/

621 Kelion, L. (1 September, 2020). Coronavirus: Apple iPhones can contact-trace without Covid app. *BBC News*. https://www.bbc.com/news/technology-53987928

minētās epizodes spilgti parāda ASV tehnoloģiju gigantu ietekmi uz valdību lēmumiem,[622] strauji pieaugošo valstu atkarību no tiem, ieviešot plaša mēroga digitālos risinājumus sabiedrības interesēs, un tas rada tālākus jautājumus par šo lielo tehnoloģiju uzņēmumu varas ierobežošanu un digitālās suverenitātes aizsardzību.

Neatkarīgi no izvēlētā tehnoloģiskā risinājuma galvenais jautājums, kas jāuzdod saistībā ar kontakta izsekošanas lietotnēm, kā arī ikvienu citu digitālo risinājumu izmantošanu, ir – vai šie risinājumi var palīdzēt apturēt vīrusa izplatību, proti, vai tie ir efektīvi. Šo lietotņu efektivitāte ir atkarīga no tā, cik daudz iedzīvotāju to ir lejupielādējuši un izmanto. Oksfordas Universitātes pētnieki norāda, ka vismaz 60 % iedzīvotāju būtu jāizmanto lietotne, lai tā būtu efektīva.[623] Lietotnes, kas vairs nav efektīvas, ir jāuzlabo, vai to darbība jāpārtrauc. Ja digitālās novērošanas tehnoloģijas ir neefektīvas, tās kļūst nevajadzīgas, un tādējādi arī to izmantošana ir uzskatāma par prettiesisku. Šo digitālo tehnoloģiju efektivitāte, lai palīdzētu ierobežot Covid-19 izplatību, tā arī netika pierādīta.[624]

Kontaktu izsekošanas lietotņu un citu jauno tehnoloģiju ietekmes, efektivitātes un nepieciešamības novērtēšana un stingra pārraudzība gan pandēmijas laikā, gan pēc tās ir būtiska, ne tikai lai palīdzētu aizsargāt cilvēktiesības, bet arī lai masveida novērošanas pasākumi nekļūtu par jauno normu. Tas, cik ātri plašs ieinteresēto dalībnieku – zinātnieku, tehnoloģiju uzņēmumu, civilo sabiedrības organizāciju, starptautisko organizāciju – loks tika iesaistīts un sadarbojās, lai izstrādātu standartus kontaktu izsekošanas lietotņu ieviešanai un lai izvērtētu to darbību, varētu būt labs piemērs praksei, kā varētu tikt izvērtēta arī citu jauno tehnoloģiju atbilstība regulējumam. Daudzas prasības, kas izkristalizējās diskusiju laikā, piemēram, efektivitāte, brīvprātīgums, ietekmes novērtējums, neatkarīga uzraudzība, termiņa ierobežošana, atbildība, ir būtiski attiecināt arī uz mākslīgā intelekta novērošanas tehnoloģijām.

Nākamajā nodaļā sniegtas konkrētas politikas rekomendācijas, vēršot uzmanību uz nepieciešamību ne tikai nodrošināt atbildības un uzraudzības prasības, bet arī paredzēt stingrus ierobežojumus šo tehnoloģiju izmantošanai.

622 Sk. Ilves, I. (16 June, 2020). Why are Google and Apple dictating how European democracies fight coronavirus? *The Guardian.* https://www.theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-european-democracies-coronavirus

623 Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown. (16 April, 2020). *University of Oxford.* https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

624 Sk., piemēram, European Commission (2020), Mobile applications to support contact tracing ..

7. DAĻA

Mākslīgā intelekta novērošanas regulējuma izstrāde un sarkanās līnijas: politikas rekomendācijas

Grāmatas iepriekšējās nodaļās atklāts, cik lielu apdraudējumu mākslīgā intelekta novērošanas tehnoloģijas rada cilvēktiesībām un demokrātijai. Tāpat parādīts, kā esošais cilvēktiesību un datu aizsardzības regulējums ir piemērojams attiecībā uz šīm tehnoloģijām, kā tas attīstās un kādus tiesiskos izaicinājumus tās rada. Šajā nodaļā sniegti vairāki ieteikumi, kā attīstīt tālāk mākslīgā intelekta regulējumu un kādi līdzekļi un aizsardzības garantijas ir jāievieš praksē, lai nodrošinātu atbildīgu un uzticamu mākslīgā intelekta tehnoloģiju izmantošanu, kas novērstu to radītos riskus un aizsargātu cilvēktiesības, demokrātiju un tiesiskumu.

Vispirms atklāts, ka mākslīgā intelekta regulējums nav saistīts tikai ar ētikas principiem, un uzsvērts, ka šī regulējuma turpmākajā attīstībā visnozīmīgākās ir cilvēktiesības. Pēc tam pamatots, ka, lai novērstu mākslīgā intelekta novērošanas tehnoloģiju radītos riskus, ir nepieciešams steidzami pieņemt mākslīgā intelekta tiesisko regulējumu, kas cita starpā noteiktu šo tehnoloģiju izmantošanas sarkanās līnijas. Tālāk ieteikti vairāki būtiski mehānismi un aizsardzības garantijas: mākslīgā intelekta ietekmes novērtējums, neatkarīga uzraudzība, sabiedrības līdzdalība, pārredzamības un informēšanas prasības. Nobeigumā vērsta uzmanība – lai masveida novērošana nekļūtu par jauno normu, ir stingri jāuzrauga to novērošanas tehnoloģiju izmantošana, kuras valstis strauji ieviesa cīņā ar Covid-19.

7.1. No ētikas principiem līdz to ieviešanai praksē

Diskusijās par mākslīgā intelekta regulējumu līdz šim lielākā uzmanība ir pievērsta ētikas principiem. Pētījumi, kuros ir salīdzinātas un analizētas mākslīgā intelekta ētikas vadlīnijas, ko pieņēmušas starptautiskās organizācijas, nevalstiskās un profesionālās organizācijas, kā arī tehnoloģiju uzņēmumi, parāda, ka lielā mērā pastāv konverģence starp tajās noteiktajiem ētiskajiem principiem, piemēram, privātumu, atbildību, pārredzamību, cilvēka kontroli pār tehnoloģijām, taisnīgumu un nediskrimināciju.[625]

Vienlaikus ir arī konstatēts, ka šīs vadlīnijas, kuru skaits jau 2020. gadā bija tuvu simtam un turpina pieaugt, lielākoties sniedz vispārējus ieteikumus un

625 Sk. Fjeld, et al. (2020), Principled Artificial Intelligence; Jobin, Ienca, Vayena (2019), The global landscape of AI ethics guidelines.

priekšlikumus, bet neparedz praktiskus izpildes mehānismus.[626] Turklāt pastāv būtiskas atšķirības, kā šie principi tiek interpretēti un īstenoti praksē.[627] Ir daudz politiska un tiesiska rakstura neskaidrību, un tiek piedāvāti dažādi un bieži vien pretrunīgi pasākumi, kā praktiski nodrošināt uz ētikas principiem balstīta mākslīgā intelekta attīstību.[628]

Šī atšķirīgā izpratne par dažādiem principiem, tostarp privātuma un datu aizsardzības prasībām, un to piemērošanu praksē, par to, kā samērojamas konkurējošas intereses, traucē vienoties par globālu regulējumu.[629] Organizācijas, kas uzņemas vadību mākslīgā intelekta regulējuma izstrādē, var to veidot atbilstīgi savām interesēm, un tām ir labākas iespējas pielāgot regulējumu savām vajadzībām. Ņemot vērā mākslīgā intelekta ētikas un satura neskaidrību un elastību, patlaban ikviens šo regulējumu var veidot ar sev vēlamo ētisko saturu.[630]

Turklāt starp dažādiem ētikas principiem ir iespējami konflikti, kas prasa vienotu pieeju, kā tos risināt. Konflikts var pastāvēt, piemēram, starp privātuma un pārredzamības prasību. Viena no pretrunām rodas starp prasību izvairīties no iespējamā kaitējuma un prasību līdzsvarot riskus un ieguvumus. Turklāt risku un ieguvumu novērtējums var novest pie atšķirīgiem rezultātiem atkarībā no interesēm, kuras tiek pārstāvētas. Sabiedrības intereses var netikt ņemtas vērā, līdzsvarojot konkurējošas prasības, piemēram, gadījumos, kad tiek ietekmētas ētiskas vērtības, bet tajā pašā laikā tiek iegūtas arī ekonomiskas vai politiskas priekšrocības.[631] Ja šādi konflikti netiek atrisināti, var būt apgrūtināti centieni izstrādāt globālu mākslīgā intelekta ētikas regulējumu. Bez būtiskām izmaiņām regulējumā ētikas principu ieviešana praksē paliks konkurējošs, nevis sadarbības process.[632]

Kā tika atklāts grāmatas piektajā nodaļā, ir izstrādāta plaša starptautiskā tiesu prakse un izveidota strukturēta sistēma konfliktu risināšanai starp konkurējošām cilvēktiesībām un sabiedrības interesēm, piemēram, privātuma un drošības

626 Hagendorff, T. (2020). The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds & Machines,* 30, 99–120. https://doi.org/10.1007/s11023-020-09517-8

627 Ryan, M., Stahl, B. C. (2020). Artificial Intelligence Ethics Guidelines for Developers and Users: Clarifying Their Content and Normative Implications, *Journal of Information, Communication and Ethics in Society,* 19(1). https://doi.org/10.1108/JICES-12-2019-0138

628 Jobin, Ienca, Vayena (2019), The global landscape of AI ethics guidelines.

629 Ibid.

630 Yeung, K., Howes, A., Pogrebna, G. (2020). AI Governance by Human Rights–Centered Design, Deliberation, and Oversight: An End to Ethics Washing, p. 80. In: Dubber, M. D., Pasquale, F., and Das, S. (eds.), *The Oxford Handbook of Ethics of AI*, 75–106. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190067397.013.5

631 Mittelstadt (2019), Principles alone cannot guarantee ethical AI.

632 Ibid.

interesēm. Konfliktu risināšana starp dažādām cilvēktiesībām ir labi saprotama, un to plaši piemēro cilvēktiesību juristi, jo tā veido būtisku daļu no cilvēktiesību piemērošanas prakses. Kā tika atklāts iepriekš grāmatas piektajā nodaļā, pastāv vairāki pamatnosacījumi cilvēktiesību ierobežošanai, it īpaši prasība, ka ierobežojumiem ir jābūt skaidri noteiktiem likumā un tie nevar pārsniegt minimumu, kas ir nepieciešams, lai sasniegtu konkrēto sabiedrības mērķi.[633] Šī sistēma būtu piemērojama arī attiecībā uz konfliktu risināšanu starp ētikas normām, kas prasa samērot pretējās intereses, izvērtējot to nepieciešamību un proporcionalitāti.

Mākslīgā intelekta attīstību nevar balstīt vienīgi uz mākslīgā intelekta ētikas principiem.[634] Vienoties par kopīgām un starptautiski atzītām morāles normām un ideāliem ir svarīgi, jo tie tiecas uz pilnību, iedvesmo uz rīcību, iezīmē skaidrāku virzību tāda mākslīgā intelekta attīstībai, kas kalpotu cilvēcei un sabiedrībai un sniegtu ieguvumus. Tomēr ar tiem nav pietiekami. Vienlaikus ir jānosaka arī metodes un līdzekļi, kas ļauj ētikas vērtības un principus ieviest praksē.

Tiesiskās prasības ir svarīgs instruments, lai nodrošinātu atbildību un ieviestu praksē ētikas principus un sociālās vērtības. Lai gan pastāv pamatotas domstarpības par to, kas ir ētiska rīcība katrā konkrētā gadījumā, ir jādefinē saskaņotu normu kopums, kas veido minimālās prasības, kuras jāievēro, lai mākslīgā intelekta sistēmu izstrādi, ieviešanu un izmantošanu varētu atzīt par ētisku un likumīgu.[635] Ir nepieciešams izstrādāt skaidru tiesisko regulējumu, kas atbilstu ētikas normām un cilvēktiesībām.

Juridiski saistošas prasības un pienākumi ir īpaši svarīgi gadījumos, kad mākslīgā intelekta sistēmas var radīt augstu risku un būtisku apdraudējumu. Šādā gadījumā nepietiek ar brīvprātīgām prasībām, lai novērstu radītos riskus. Skaidrs tiesiskais regulējums ir sevišķi nepieciešams attiecībā uz mākslīgā intelekta masveida novērošanas tehnoloģiju izstrādi, ieviešanu un izmantošanu, ņemot vērā to radīto būtisko apdraudējumu.

Cilvēktiesības ir pamatā ētikas principiem. To ievērošana demokrātiskā un tiesiskā sabiedrībā ir visdrošākais pamats abstrakto ētikas principu un vērtību noteikšanai. Cilvēktiesības ietver skaidri definētus jēdzienus un uzliek skaidrus juridiskus pienākumus, kas ir noteikti starptautiskajos tiesību aktos. Starptautiskie cilvēktiesību standarti piedāvā visprecīzāko ētikas normu kopumu mākslīgā intelekta sistēmām.[636] Vienlaikus arī ētikas principu formulēšana papildina cilvēktiesību standartus. Šie principi var palīdzēt saprast, kā mākslīgā intelekta izstrāde, ieviešana un izmantošana varētu ietekmēt cilvēktiesības un to pamatā

633 Yeung, Howes, Pogrebna (2020), AI Governance by Human Rights .., p. 83.

634 Mittelstadt (2019), Principles alone cannot guarantee ethical AI.

635 Yeung, Howes, Pogrebna (2020), AI Governance by Human Rights .., p. 80.

636 Ibid., pp. 80–81.

esošās vērtības, likt apsvērt ne tikai to, kā mēs tehnoloģijas varētu izmantot, bet gan arī to, kādā veidā mums tehnoloģijas būtu jāizmanto, lai tās sniegtu labumu, nevis apdraudētu sabiedrību.[637]

7.2. Cilvēktiesības kā mākslīgā intelekta regulējuma stūrakmens

Cilvēktiesības ir stūrakmens ētiskai un uz cilvēku vērstai mākslīgā intelekta regulējuma turpmākai attīstībai. Starptautiskās cilvēktiesības veido starptautisku tiesību kopums, kā arī reģionālās cilvēktiesību sistēmas, kas ir izveidotas pēdējo 70 gadu laikā visā pasaulē. Kā starptautisks pārvaldības mehānisms cilvēktiesību tiesiskais regulējums ir paredzēts, lai izveidotu globālus standartus, t. i., normu kopumu un atbildības mehānismus, kas nosaka veidu, kā pret cilvēkiem ir jāizturas. Cilvēktiesības nodrošina universālu obligāto standartu kopumu, kas cita starpā balstās uz cilvēka cieņas, autonomijas, vienlīdzības un tiesiskuma vērtībām. Šie standarti un ar tiem saistītie tiesiskie mehānismi valstīm rada juridiskus pienākumus ievērot, aizsargāt un īstenot cilvēktiesības. Tie arī pieprasa, lai personas, kurām viņu tiesības ir liegtas vai pārkāptas, varētu saņemt efektīvu tiesisko aizsardzību. Satversmes tiesa ir uzsvērusi, ka personas pamattiesību aizsardzība ir viens no demokrātiskas tiesiskas valsts nozīmīgākajiem pienākumiem.[638] Tas ir pilnībā attiecināms arī uz mākslīgo intelektu. Cilvēktiesību aizsardzība ir viens no būtiskākajiem valsts pienākumiem arī mākslīgā intelekta laikmetā.

Cilvēktiesības veido mākslīgā intelekta regulējuma pamatu, un tām ir primāra nozīme turpmākā starptautiskā un ES mākslīgā intelekta tiesiskā regulējuma attīstībā. Tas uzsvērts vairāku starptautisko organizāciju dokumentos, piemēram, Eiropas Padomes[639], ES[640] un UNESCO[641] mākslīgā intelekta ētikas vadlīnijās, kuras atsaucas uz starptautiskajiem cilvēktiesību dokumentiem. Arī tiesību zinātnieki ir uzsvēruši, ka cilvēktiesībām ir jābūt mākslīgā intelekta regulējuma pamatā.[642] Vadlīnijās noteiktie ētikas principi ir balstīti uz konkrētām cilvēktiesībām, to aizsardzību un veicināšanu, tostarp tiesībām uz vienlīdzību, nediskriminācijas principu, biedrošanās brīvību, tiesībām uz privāto dzīvi, ekonomiskajām, sociālajām un kultūras tiesībām, piemēram, tiesībām uz izglītību

637 Sk. AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

638 Satversmes tiesas 2012. gada 20. aprīļa spriedums lietā Nr. 2011-16-01, 9. punkts.

639 Council of Europe, CAHAI Secretariat (2020). Towards regulation of AI systems.

640 Eiropas Komisija (2020), Baltā grāmata par mākslīgo intelektu.

641 UNESCO, AHEG (2020), Outcome document: First Draft of the Recommendation on the Ethics of Artificial Intelligence.

642 Sk., piemēram, Mantelero (2020), Regulating AI within the Human Rights Framework.

un tiesībām uz veselību. Piemēram, ētikas princips "kaitējuma novēršana" prasa aizsargāt cilvēka cieņu, kā arī visas pārējās cilvēktiesības. Tajā pašā laikā CAHAI ir vērsusi uzmanību, ka daudzas no vadlīnijām konkrēti nenorāda uz nepieciešamību veicināt cilvēktiesības, kā arī nebrīdina par cilvēktiesību pārkāpumiem, ko var radīt mākslīgā intelekta sistēmu izstrāde un ieviešana, līdz ar to ir steidzami nepieciešams vērst lielāku uzmanību uz cilvēktiesību ietekmi.[643]

Cilvēktiesību regulējuma izmantošanai mākslīgā intelekta kontekstā ir daudzas priekšrocības: ir izveidotas institūcijas, judikatūra, tiek izmantota universāla valoda un cilvēktiesības ir starptautiski atzītas. Laika gaitā ir izveidota plaša starptautiska, reģionāla un nacionāla līmeņa cilvēktiesību aizsardzības sistēma. Tā sastāv no starptautiskām organizācijām, tiesām, nevalstiskām organizācijām un citām institūcijām, kurās var vērsties cilvēktiesību pārkāpuma gadījumā un izmantot tiesiskās aizsardzības līdzekļus. Cilvēktiesības pamatojas kopīgās vērtībās, kas kā juridiski saistošas tiesību normas tiek interpretētas un piemērotas konkrētās situācijās starptautiskajā, reģionālajā un nacionālajā tiesu praksē. Cilvēktiesības nodrošina universālu valodu globāliem jautājumiem. Cilvēktiesību aizsardzības institūcijas aktīvi piedalās diskusijās par mākslīgā intelekta vietu sabiedrībā kopā ar citām ieinteresētajām pusēm, kas ir tieši iesaistītas mākslīgā intelekta izstrādē un izmantošanā. Turklāt cilvēktiesības ir starptautiski atzītas un ietvertas juridiski saistošos tiesību aktos.[644]

OECD norāda, ka cilvēktiesībās balstītā pieeja mākslīgajam intelektam var palīdzēt identificēt riskus, it īpaši augstus riskus, prioritātes, neaizsargātās un mazāk aizsargātās grupas un nodrošināt tiesiskās aizsardzības līdzekļus. Cilvēktiesības var palīdzēt noteikt kaitējuma risku, piemēram, ja tiek veikts ietekmes uz cilvēktiesībām novērtējums, kas kā atsevišķs mehānisms aplūkots nodaļas turpinājumā. Cilvēktiesības kā minimālie standarti nosaka pamatprasības, kuras nedrīkst pārkāpt. Piemēram, regulējot izteiksmes brīvību sociālajos tīklos, cilvēktiesības palīdz noteikt naida runu kā sarkano līniju. Līdzīgā veidā cilvēktiesības, to skaitā cilvēka cieņa, nediskriminācijas princips, privātums un datu aizsardzība, būtu jāņem vērā, nosakot sejas atpazīšanas un citu novērošanas tehnoloģiju izmantošanas sarkanās līnijas, kas tālāk analizētas atsevišķi. Cilvēktiesības var palīdzēt noteikt neaizsargāto iedzīvotāju vai riska grupas, vai kopienas mākslīgā intelekta sistēmu izmantošanas gadījumā. Jau iepriekš tika atklāts, ka sievietes un atsevišķas etniskās grupas var būtiski vairāk skart sejas atpazīšanas tehnoloģiju izmantošana. Cilvēktiesības kā tiesību normas, kas rada pienākumus, var palīdzēt tiem, kuru tiesības tiek pārkāptas. Tās garantē personām tiesiskās

643 Council of Europe, CAHAI Secretariat (2020). Towards regulation of AI systems.

644 Access Now. (2018). Human rights in the age of artificial intelligence. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

aizsardzības līdzekļus, un tie var būt, piemēram, darbības pārtraukšana, jaunu procesu vai politikas izstrāde, atvainošanās vai naudas kompensācija.[645]

OECD ir vērsusi uzmanību, ka ir arī vairāki būtiski izaicinājumi, lai īstenotu uz cilvēktiesībām balstīto pieeju attiecībā uz mākslīgo intelektu. Cilvēktiesības ir vairāk vērstas uz valstīm, nevis privātiem dalībniekiem, tajā pašā laikā tieši privātā sektora dalībniekiem ir galvenā loma mākslīgā intelekta sistēmu izstrādē un ieviešanā. Vairāku starpvaldību iniciatīvu mērķis ir novērst plaisu starp valsts un privāto sektoru.[646] Privātie uzņēmumi var nebūt ieinteresēti aizsargāt cilvēktiesības, īpaši tad, ja tādējādi var tikt samazināta peļņa. Tomēr arvien vairāk tiek atzīts, ka cilvēktiesību aizsardzība sniedz labumu arī uzņēmumu biznesa interesēm. Vēl viens izaicinājums ir tas, ka cilvēktiesību aizsardzība ir saistīta ar jurisdikciju. Parasti prasītājam ir jāpierāda tiesiskais statuss noteiktā jurisdikcijā, un tas var nebūt efektīvi un radīt grūtības gadījumos, kad ir iesaistīti lieli starptautiski uzņēmumi un mākslīgā intelekta sistēmas, kas aptver vairākas jurisdikcijas. Vēl viens trūkums ir, ka cilvēktiesības ir labāk piemērotas, lai samazinātu būtisku kaitējumu nelielam skaitam cilvēku, nevis novērstu kaitējumu kolektīvām interesēm. Individuālā ceļā ir grūtāk apstrīdēt mākslīgā intelekta sistēmas, to skaitā novērošanas sistēmas, un to radīto ietekmi, kas apdraud cilvēktiesības un brīvības. Ir nepieciešama vienota un koordinēta rīcība, lai aizsargātu privātumu un autonomiju kā sabiedrības labumu. Pretējā gadījumā pastāv dziļš šo sistēmu konflikts ar demokrātijas, brīvības un vienlīdzības principu.[647] Arī dažas vispārējas mākslīgā intelekta regulējuma problēmas, piemēram, pārredzamība un izskaidrojamība, attiecas uz cilvēktiesību jautājumiem. Bez pārredzamības ir grūti noteikt, vai ir pārkāptas cilvēktiesības.[648]

Cilvēktiesības kā juridiski saistošs normu kopums kopā ar citiem saistītiem tiesiskiem un institucionāliem mehānismiem veido pamatu, lai nodrošinātu ētisku un uz cilvēku vērstu mākslīgā intelekta attīstību un izmantošanu. Jau tagad mākslīgā intelekta attīstībai un izmantošanai ir jāatbilst starptautiskajiem un ES cilvēktiesību dokumentiem, īpaši ECTK un Hartai, kā arī valstu nacionālajiem tiesību aktiem, īpaši konstitūcijām, kurās parasti ir iekļautas cilvēktiesību

645 OECD. (2019). Artificial Intelligence in Society. https://www.oecd.org/publications/artificial-intelligence-in-society-eedfee77-en.htm

646 Nesenie starpvaldību instrumenti, piemēram, ANO Uzņēmējdarbības un cilvēktiesību pamatprincipi, atzīmē privāto dalībnieku lomu cilvēktiesību kontekstā, tai skaitā paredzot to atbildību par cilvēktiesību ievērošanu. Sk. OHCHR. (2011). Guiding Principles on Business and Human Rights. Implementing the United Nations "Protect, Respect and Remedy" Framework. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

647 Lewandowsky, Smillie, Garcia, et al. (2020), Technology and Democracy.

648 OECD (2019), Artificial Intelligence in Society.

normas. Kā tika atklāts grāmatas otrajā nodaļā, cilvēktiesību normas jau šobrīd ir piemērojamas un paredz juridiski saistošas prasības attiecībā uz mākslīgā intelekta novērošanas sistēmām. Daudzas prasības, kas noteiktas ētikas vadlīnijās, jau ir ietvertas gan cilvēktiesību, gan citos tiesību aktos.

Eiropas cilvēktiesību aizsardzības sistēmā varētu tikt izveidots uz cilvēktiesībām balstīts mākslīgā intelekta regulējums, kas kalpotu par paraugu pārējai pasaulei. ES pamatā ir cilvēka cieņas, brīvības, demokrātijas, tiesiskuma un cilvēktiesību ievērošanas vērtības. ES varētu radīt "zelta standartu" regulas formā cilvēktiesībās balstītam mākslīgā intelekta regulējumam, kas būtu tiešā veidā piemērojama visās dalībvalstīs, līdzīgi kā ES datu aizsardzības noteikumi. Arī Eiropas Padome varētu izstrādāt skaidru uz cilvēktiesībām, tiesiskumu un demokrātiskām vērtībām balstītu regulējumu, pieņemot jaunu saistošu tiesisko instrumentu, piemēram, pamatkonvenciju.

Izstrādājot mākslīgā intelekta tiesisko regulējumu, cilvēktiesību normas būtu attīstāmas tālāk, skaidri nosakot to piemērošanu attiecībā uz konkrētiem to izmantošanas gadījumiem. Šīs grāmatas iepriekšējās nodaļās veiktā analīze atklāj, ka ir nepieciešams ierobežot un stingri regulēt valstu masveida novērošanas praksi, kas īstenota, izmantojot mākslīgā intelekta tehnoloģijas, lai tā atbilstu cilvēktiesībām, un ir nepieciešams noteikt skaidras robežas un atbildības mehānismus. Atkāpšanās no cilvēktiesībām īpašos izņēmuma apstākļos, piemēram, drošības nolūkos, būtu atļaujama, tikai ja tas ir stingri jeb absolūti nepieciešams un ievērojot ierobežošanas nosacījumus.

Pašreizējā uz cilvēktiesībām balstītā pieeja mākslīgajam intelektam ir jāpilnveido, lai izvairītos no vispārēju politikas ieteikumu noteikšanas vai tādu vispārīgu principu atkārtošanas, kuriem trūkst pienācīgas kontekstualizācijas, piemēram, nediskriminācija un pārredzamība, tas ir izšķiroši jebkuram normatīvajam regulējumam. Tādējādi turpmākajam mākslīgā intelekta regulējumam jābūt balstītam uz esošajiem cilvēktiesību instrumentiem, bet šim regulējumam vajadzētu arī spēt pielāgot un kontekstualizēt šo tiesību piemērošanu un novērst trūkumus, ko rada tiesību akti, kas izstrādāti pirms mākslīgā intelekta laikmeta.[649]

Kā tika atklāts iepriekš, mākslīgā intelekta sistēmu izmantošana var būtiski aizskart cilvēktiesības, īpaši tiesības uz privātumu un datu aizsardzību, radīt aizspriedumus un diskrimināciju. Līdzās cilvēktiesību riskiem šīm tehnoloģijām ir plašāka ietekme uz tiesiskumu un demokrātiju, un to ir grūti paredzēt vai izmērīt.

Vācijas tiesību zinātnieks Pauls Nemics (*Paul Nemitz*) norāda, ka cilvēktiesības, demokrātija un tiesiskums ir Rietumu liberālo konstitūciju pamatelementi, mūsu konstitucionālās ticības "trinitārā formula". Šie principi ir augstākais likums – visas valdības, likumdevēju un sabiedrībā notiekošie procesi tiek vērtēti,

649 Mantelero (2020), Regulating AI within the Human Rights Framework, p. 480.

vadoties no tiem. Ņemot vērā mākslīgā intelekta paredzamo straujo izplatību mūsdienu sabiedrībā, ir nepieciešams uzdot jautājumu, kā šīs jaunās tehnoloģijas veidot tā, lai atbalstītu konstitucionālo "trinitāro formulu" un to nostiprinātu, nevis vājinātu. Šeit piedāvātā atbilde – mums ir nepieciešama jauna tehnoloģiju un biznesa attīstības kultūra mākslīgā intelekta laikmetam, kas integrē tiesiskumu, demokrātiju un cilvēktiesības.[650] Atrast veidus, kā jaunās tehnoloģijas attīstīt un ieviest tikai tā, lai aizsargātu cilvēka brīvību un cieņu, kā arī konstitucionālās demokrātijas pamatus, proti, demokrātiju, tiesiskumu un cilvēktiesības, ir mūsu laika izaicinājums.[651] Lai arī pašreizējais Eiropas cilvēktiesību, privātuma un datu aizsardzības regulējums ir būtisks, tas nav pietiekams, lai novērstu visus riskus, ko rada mākslīgais intelekts. Jaunie izaicinājumi prasa jauna regulējuma izstrādi globālā līmenī, Eiropas – ES un Eiropas Padomes – līmenī, kā arī nacionālā līmenī.

7.3. Jauna mākslīgā intelekta tiesiskā regulējuma nepieciešamība

Jauna mākslīgā intelekta regulējuma izstrādi pamato nepieciešamība novērst iespējamo kaitējumu, ko mākslīgā intelekta sistēmu izmantošana var radīt. Brūss Šneiers salīdzina jauno tehnoloģiju attīstību ar lidmašīnu ieviešanu. Mūsdienās, kad kāpjam lidmašīnā, mēs pamatā jūtamies droši, ka lidojums beigsies labi, bet sākumā lidmašīnas nebija drošs pārvietošanās līdzeklis, un ar tām lidot bija bīstami. 1972. gadā avarēja 72 lidmašīnas un bojā gāja vairāk nekā 2000 cilvēku. Tas, kas mainījās, bija lidmašīnu drošības regulējums. Pagāja gadu desmiti, valdības noteica dažāda veida uzlabojumus lidmašīnu dizainam, lidojumu procedūrām, pilotu apmācībām utt. Tagad lidmašīnas ir drošs veids ceļošanai.[652]

Līdzīgā veidā mēs mūsdienās arvien skaidrāk redzam, kādu kaitējumu var radīt jaunās tehnoloģijas un mākslīgais intelekts, un arvien vairāk apzināmies nepieciešamību izveidot stingru regulējumu, kas to novērstu. Tajā pašā laikā jaunās tehnoloģijas atšķirībā no lidmašīnām var izmantot ļoti dažādos un pat grūti prognozējamos veidos, kā arī dažādās jomās, un tas apgrūtina skaidra regulējuma izveidi, turklāt prasa komplicētu pieeju, apvienojot dažādus regulējuma veidus.

650 Nemitz, P. (2018). Constitutional Democracy and Technology in the Age of Artificial Intelligence. *Philos. Trans. R. Soc. A-Math. Phys. Eng. Sci.,* 376(2133). https://doi.org/10.1098/RSTA.2018.0089

651 Nemitz, P. (2018). Profiling the European Citizen: Why today's democracy needs to look harder at the negative potential of new technology than at its positive potential. In: Bayamlioğlu, E., Baraliuc, I., Janssens, L. u. a. (eds.), *Being Profiled: Cogitas Ergo Sum. 10 Years of Profiling the European Citizen.* Amsterdam: Amsterdam University Press, pp. 8–11. https://doi.org/10.2307/j.ctvhrd092.3

652 Sk. Schneier (2016), *Data and Goliath* .., p. 144.

Tiesiskajam regulējumam ir vairāki trūkumi. Viens no lielākajiem izaicinājumiem – tehnoloģijas attīstās daudz ātrāk, nekā tiek pieņemti jauni likumi. Tiesību aktu pieņemšanas process ir ilgs, tāpēc tas netiek līdzi straujajai tehnoloģiju attīstībai. Tiesību normas to pieņemšanas brīdī bieži vien jau vairs neatbilst esošajām jaunākajām tehnoloģiju attīstības tendencēm. Līdzīgi arī esošie tiesiskie instrumenti, kas pieņemti pirms mākslīgā intelekta sistēmu plašas izmantošanas, mēdz mazināt to efektivitāti un neļauj adekvāti un konkrēti reaģēt uz mākslīgā intelekta sistēmu izaicinājumiem, jo nav pielāgoti to specifikai.[653]

Vēl viens arguments, ko bieži izmanto privātie uzņēmumi, iebilstot pret jaunām tiesiskām prasībām, – tiesiskais regulējums var kavēt inovāciju un tehnoloģiju attīstību. Daudzos gadījumos tiesiskais regulējums var nebūt piemērotākais līdzeklis. Pastāv arī citi rīcības veidi, kas konkrētu tehnoloģiju regulēšanai var būt piemērotāki salīdzinājumā ar juridiski saistošiem noteikumiem. Piemēram, ētikas noteikumi vai sertifikācija var definēt un palīdzēt īstenot prasības jauno tehnoloģiju izstrādei un izmantošanai, kā arī var palīdzēt panākt, lai sabiedrība tām uzticas. Tomēr pašregulācija nav pietiekama. Tā nevar efektīvi darboties gadījumā, kad tehnoloģiju izmantošana var radīt kaitējumu. Būtu naivi cerēt, ka uzņēmumi, kas gūst peļņu no tehnoloģiju izstrādes un izmantošanas, paši tās regulēs un ierobežos to izmantošanu. Regulējumam ir jābūt samērīgam, proporcionālam, elastīgam, lai veicinātu inovāciju un tehnoloģiju attīstību un sabiedrības uzticību. Savukārt stingrs tiesiskais regulējums, kas nosaka ierobežojumus un sankcijas, būtu jāizmanto gadījumos, kad jaunās tehnoloģijas var radīt kaitējumu cilvēkiem, viņu tiesībām, drošībai, sabiedrības vērtībām un demokrātijai, kā arī var radīt cita veida būtisku kaitējumu, lai panāktu, ka tas tiek novērsts.

Eiropas Padome vērš uzmanību – lai gan attiecībā uz mākslīgo intelektu nepastāv tiesiskais vakuums, tomēr eksistē tiesiskas nepilnības. Pirmkārt, tiesības un pienākumi, kas minēti spēkā esošajos tiesiskajos instrumentos, īpaši cilvēktiesību normās, parasti tiek formulēti plaši vai vispārīgi. Tas pats par sevi nav problemātiski, tomēr dažos gadījumos var būt grūtības tos interpretēt attiecībā uz mākslīgā intelekta sistēmām. Turklāt tie nepārprotami nerisina dažus ar mākslīgo intelektu saistītus jautājumus, tādējādi traucējot to efektīvu piemērošanu situācijās, ko rada mākslīgā intelekta sistēmas. Otrkārt, vairāki būtiski principi, kas attiecas uz cilvēktiesību, demokrātijas un tiesiskuma aizsardzību mākslīgā intelekta jomā, pašlaik nav tieši tiesiski noteikti. Šīs nepilnības attiecas, piemēram, uz nepieciešamību nodrošināt pietiekamu cilvēku kontroli un uzraudzību, sistēmu tehnisko noturību, efektīvu pārredzamību un izskaidrojamību, it īpaši, ja mākslīgā intelekta sistēmu izmantošana rada tiesiskas vai citas būtiskas sekas

653 Council of Europe, CAHAI (2020), Feasibility Study.

personām. Treškārt, pašreizējie instrumenti arī nepievērš pietiekamu uzmanību pasākumiem, kas jāveic sistēmu izstrādātājiem un lietotājiem, lai nodrošinātu šo sistēmu efektivitāti ikreiz, kad tās var ietekmēt cilvēktiesības, demokrātiju vai tiesiskumu, un nodrošinātu, ka tiem ir nepieciešamā kompetence vai profesionālā kvalifikācija. Šīs juridiskās nepilnības un paredzama un pamatota tiesiskā regulējuma trūkums var radīt nenoteiktību mākslīgā intelekta izstrādātājiem, piegādātājiem un lietotājiem.[654]

Arvien vairāk tiek atzīts, ka ir nepieciešams skaidrs mākslīgā intelekta tiesiskais regulējums. Kā jau tika atklāts iepriekš, Eiropas Komisija ir publicējusi MI akta priekšlikumu.[655] Arī Eiropas Padome šobrīd apsver jauna mākslīgā intelekta tiesiskā regulējuma izstrādi, kas varētu apvienot jauna saistoša tiesiskā instrumenta, piemēram, konvencijas vai pamatkonvencijas, pieņemšanu, nesaistošus tiesiskos instrumentus, kā arī nozaru jeb sektorālā tiesiskā regulējuma pilnveidošanu.[656]

Viena no jomām, kas būtu īpaši regulējama, ir automatizēto lēmumu pieņemšana, tostarp izmantojot novērošanas tehnoloģijas. Džovanni Sartors secina, ka attiecībā uz mākslīgā intelekta sistēmu izmantošanu var tikt ievēroti datu aizsardzības noteikumi un nav nepieciešamas būtiskas izmaiņas esošā datu aizsardzības regulējumā.[657] Tajā pašā laikā var tikt apgrūtināta dažu prasību īstenošana. Tāpēc būtu skaidrāk jānosaka, kā datu aizsardzības prasības, piemēram, pārredzamības prasības un prasības, kas attiecas uz automatizētu lēmumu pieņemšanu, ir piemērojamas konkrētos gadījumos.[658]

Tiesību jomas eksperti iesaka stiprināt esošās cilvēktiesības, kā arī apsvērt iespējas regulējumā noteikt pielāgotas vai pat jauna veida cilvēktiesības. Piemēram, AI HLEG dalībniece Kateleine Millere (*Catelijne Muller*) norāda, ka būtu apsveramas vairākas pielāgotas vai pat jaunas cilvēktiesības: tiesības uz cilvēka autonomiju; cilvēka uzraudzība pār mākslīgo intelektu; atsevišķas tiesības uz fizisko, psiholoģisko un morālo integritāti, ņemot vērā mākslīgā intelekta profilēšanu un emociju atpazīšanu. Tiek ieteikts arī stiprināt un pielāgot tiesības uz privātumu, lai aizsargātu pret mākslīgā intelekta masveida novērošanu un nediferencētu, sabiedrības mēroga personu novērošanu tiešsaistē, izmantojot gan personas datus, gan nepersondatus.[659] Esošās cilvēktiesību normas jau šobrīd

654 Council of Europe, CAHAI (2020), Feasibility Study.

655 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

656 Council of Europe, CAHAI (2020), Feasibility Study.

657 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

658 Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence.

659 Ibid.

ietver daudzus no minētajiem aspektiem. Šīs normas būtu pielāgojamas un konkretizējamas nākotnes mākslīgā intelekta tiesiskajā regulējumā.

Cilvēktiesību un datu aizsardzības regulējumu vajadzētu vairāk attiecināt uz kolektīvo interešu aizsardzību, uz ko ir vērsuši uzmanību daudzi tiesību zinātnieki.[660] Kā tika atklāts grāmatas 3.6. nodaļā, datu aizsardzības eksperti ir pierādījuši, ka lielo datu analītikas attīstība prasa jaunu grupu privātuma aizsardzību, veltot īpašu uzmanību algoritmiskās klasifikācijas rezultātā veidotajām grupām.[661]

Mākslīgā intelekta tiesiskais regulējums pēc iespējas ir jāpielāgo konkrētās jomas specifikai, it īpaši augsta riska jomās, tostarp tiesībaizsardzībā. Ņemot vērā, ka cilvēktiesību un datu aizsardzības tiesību akti, īpaši VDAR un Policijas direktīva, paredz svarīgas prasības attiecībā uz mākslīgā intelekta novērošanas tehnoloģiju ieviešanu un izmantošanu, būtu nepieciešams konkretizēt, kā tās ir piemērojamas attiecībā uz valsts novērošanas pasākumiem. Eiropas Padome sevišķi uzsver nepieciešamību regulēt sejas atpazīšanas tehnoloģijas. Vadlīnijas par sejas atpazīšanu mudina valstis izstrādāt un pieņemt specifiskus noteikumus, kas regulētu sejas atpazīšanas tehnoloģiju biometrisko apstrādi, kura tiek veikta tiesībaizsardzības nolūkos.[662]

Kā tika atklāts grāmatā, kaut gan esošais regulējums paredz būtiskas prasības, pašreiz spēkā esošais tiesiskais regulējums nav pietiekams, lai tiktu galā ar mākslīgā intelekta novērošanas tehnoloģiju radīto apdraudējumu. Lai novērstu šos izaicinājumus, būtiska nozīme ir arī skaidru ierobežojumu jeb sarkano līniju noteikšanai.

7.4. Sarkano līniju noteikšana

Skaidru sarkano līniju noteikšanai ir ļoti svarīga nozīme, lai novērstu tādu mākslīgā intelekta sistēmu izmantošanu, kas pārkāpj cilvēktiesības. Tiesiski noteiktiem ierobežojumiem ir jābūt neatņemamai uz cilvēktiesībām balstīta mākslīgā intelekta tiesiskā regulējuma sastāvdaļai. Gan zinātnieki, gan pilsoniskās sabiedrības organizāciju pārstāvji arvien vairāk mudina noteikt skaidrus normatīvus ierobežojumus tāda mākslīgā intelekta izmantošanai, kas ir pretrunā cilvēktiesībām.

660 Mantelero, A. (2017). Regulating Big Data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer Law & Security Review,* 33, pp. 584–602.

661 Sk., piemēram, Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. *Philosophy & Technology*, 30(4), pp. 475–494. https://doi.org/10.1007/s13347-017-0253-7

662 Council of Europe (2021), .. Convention 108.

Turīnas Politehniskās universitātes tiesību zinātnieks, datu ētikas un datu aizsardzības eksperts asociētais profesors Alesandro Mantelero vērš uzmanību, ka cilvēka cieņai un cilvēktiesībām ir centrālā nozīme mākslīgā intelekta izmantošanā. Viņš rosina ieviest aizliegumus konkrētām mākslīgā intelekta tehnoloģijām, kuras tiek izstrādātas veidā, kas ir pretrunā ar cilvēktiesībām, demokrātiju un tiesiskumu.[663]

Oksfordas Universitātes asociētā profesore Karisa Velisa grāmatā "Privātums ir vara" (*Privacy is Power* – angļu val.) mudina stingri ierobežot valsts novērošanu, norādot, ka valsts iestādēm nav jāveic masveida novērošana, lai iedzīvotāji būtu drošībā. Datu vākšana un analīze nedrīkstētu notikt bez ordera, un tā var notikt tikai nepieciešamības gadījumā. Tai ir jābūt mērķtiecīgai, pretstatā masveida novērošanai, kā arī proporcionālai. Zinātniece uzskata, ka dažas no novērošanas tehnoloģijām ir tik bīstamas un tik piemērotas ļaunprātīgai izmantošanai, ka būtu labāk tās aizliegt visas kopā, tāpat kā mēs aizliedzam dažus ieročus. Mums vajadzētu apsvērt iespēju aizliegt sejas atpazīšanu, kā arī gaitas un sirdspukstu atpazīšanu un citas tehnoloģijas, kas iznīcina anonimitāti, jo tie ir ideāli instrumenti apspiešanai.[664]

Arvien skaļāk normatīvi noteikt mākslīgā intelekta izmantošanas sarkanās līnijas pieprasa arī cilvēktiesību aizstāvības organizācijas. 2021. gada 21. janvārī EDRi kopā ar 60 pilsoniskās sabiedrības organizācijām iesniedza Eiropas Komisijai atklātu vēstuli, kurā aicina ieviest sarkanās līnijas gaidāmajā mākslīgā intelekta regulējuma priekšlikumā.[665] Tās aicina noteikt normatīvos ierobežojumus tāda mākslīgā intelekta izmantošanai, kas nepamatoti ierobežo cilvēktiesības. Vēstulē norādīts, ka papildus VDAR stingrai ievērošanai un tādiem aizsardzības pasākumiem kā ietekmes uz cilvēktiesībām novērtējums, programmatūras pārredzamība un datu kopuma pieejamība publiskai pārbaudei, ir svarīgi, lai topošajā tiesību akta priekšlikumā tiktu noteikti skaidri ierobežojumi, kas nosaka, ko var un ko nevar uzskatīt par likumīgu mākslīgā intelekta izmantošanu, lai nepārprotami risinātu vairākus jautājumus. Tie ir: biometriskā masveida novērošana un publisko vietu uzraudzība; strukturālā diskriminācija, atstumtība un kolektīvā kaitējuma saasināšana; tādu svarīgu pakalpojumu kā veselības aprūpe un sociālie pakalpojumi ierobežošana un diskriminējoša piekļuve; darbinieku novērošana un darba ņēmēju pamattiesību pārkāpumi; taisnīgas tiesas un procesuālo tiesību

663 Mantelero (2020), Regulating AI within the Human Rights Framework, p. 501; sk. arī Kindt, E. (2020). A First Attempt at Regulating Biomentric Data in the European Union, p. 68. In: Kak, A. (ed.). *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute, pp. 62–68. https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions

664 Véliz (2021), *Privacy Is Power*, pp. 152, 154.

665 EDRi (12 January, 2021), Re: Open letter: Civil society call for the introduction of red lines ..

pieejamības apgrūtināšana; tādu sistēmu izmantošana, kas izdara secinājumus un prognozes par mūsu vissensitīvākajām īpašībām, uzvedību un domām; īpaši būtiski – manipulācijas ar cilvēku uzvedību vai tās kontrole un ar to saistītie cilvēka cieņas, rīcības brīvības un kolektīvās demokrātijas apdraudējumi.

Vēstulē tiek mudināts it īpaši pievērst uzmanību konkrētiem mākslīgā intelekta izmantošanas veidiem, kas nav saderīgi ar demokrātisku sabiedrību un kas ir jāaizliedz vai jāierobežo mākslīgā intelekta tiesiskajā regulējumā. Pirmkārt, mākslīgā intelekta tiesību akta priekšlikumā būtu jāiekļauj nepārprotams aizliegums biometrisko datu izmantošanai bez izšķirības vai patvaļīgai mērķtiecīgai izmantošanai publiskās vai publiski pieejamās vietās, kas var izraisīt masveida novērošanu. Tas nodrošinātu, ka tiesībaizsardzības un citas valsts iestādes, kā arī privātas iestādes un uzņēmumi nevarētu ļaunprātīgi izmantot plašos izņēmumus un rīcības brīvību, kas pašlaik ir iespējama saskaņā ar vispārējiem principiem, kas nosaka biometriskās apstrādes aizliegumu. Otrkārt, Eiropas Komisija tiek mudināta tiesiskajā regulējumā noteikt ierobežojumus attiecībā uz izmantošanas veidiem, kas ir pretrunā pamattiesībām, ieskaitot mākslīgā intelekta izmantošanu robežkontrolē, prognozēšanā tiesībaizsardzības nolūkos, arī uz sistēmām, kas ierobežo piekļuvi sociālajām tiesībām un pabalstiem, un riska novērtēšanas rīkiem krimināltiesību kontekstā. Treškārt, turpmākā mākslīgā intelekta tiesību aktu un politikas izstrādē ir jāiekļauj marginalizētās un aizskartās kopienas.

EDRi pieteiktajā ES pilsoņu iniciatīvā "Atgūsti savu seju" pilsoniskās sabiedrības organizācijas pieprasa Eiropas Komisiju tiesību aktos un praksē aizliegt biometrisko masveida novērošanu. Masveida biometriskās apstrādes sistēmas nedrīkst izstrādāt, ieviest pat izmēģinājuma veidā vai izmantot publiskas vai privātas iestādes, ciktāl tās var radīt nevajadzīgu vai nesamērīgu iejaukšanos cilvēku pamattiesībās. Pierādījumi liecina, ka biometriskās masveida novērošanas izmantošana dalībvalstīs un ES aģentūrās ir izraisījusi ES datu aizsardzības tiesību pārkāpumus un nepamatoti ierobežojusi cilvēktiesības, tostarp tiesības uz privātumu, vārda brīvību, tiesības protestēt un netikt diskriminētam. Biometriskās uzraudzības, profilēšanas un prognozēšanas plaša izmantošana apdraud tiesiskumu un cilvēka pamatbrīvības. Tāpēc Eiropas Komisija tiek mudināta sagatavot tiesību aktu, kas skaidri aizliegtu biometrisko masveida novērošanu un tādējādi atbilstu spēkā esošajām ES datu aizsardzības prasībām.[666]

Nepieciešamību noteikt mākslīgā intelekta izmantošanas sarkanās līnijas ir uzsvērušas arī starptautiskās organizācijas. UNESCO Rekomendācija par mākslīgā intelekta ētiku paredz, ka mākslīgā intelekta sistēmas nedrīkst izmantot sociālai novērtēšanai vai masveida novērošanai (26. punkts).[667]

666 EDRi (17 February, 2021), New ECI calls Europeans to stand ..; European Citizens' Initiative ..

667 UNESCO (2021), Recommendation on the Ethics of Artificial Intelligence.

CAHAI 2020. gada decembra pētījumā norādīts, ka sarkanās līnijas varētu noteikt tādu mākslīgā intelekta sistēmu izmantošanai, kas tiek uzskatītas par pārāk ietekmīgām, lai tās atstātu nekontrolētas vai neregulētas, vai pat – atļautu. Var būt nepieciešams noteikt aizliegumu, pagaidu aizliegumu, stingrus ierobežojumus vai nosacījumus ārkārtas vai arī kontrolētai šādu mākslīgā intelekta sistēmu izmantošanai: sejas atpazīšanas un citu biometrisko atpazīšanas veidu izmantošanai bez izšķirības valsts vai privātajā sektorā; uz mākslīgo intelektu balstītai masveida novērošanai (izmantojot sejas, biometrisko atpazīšanu, kā arī citus mākslīgā intelekta vai identifikācijas veidus, piemēram, atrašanās vietas noteikšanas pakalpojumus, uzvedības novērošanu tiešsaistē utt.); personiskai, fiziskai vai garīgai analizēšanai, novērtēšanai, profilēšanai un uzvedības virzīšanai, izmantojot biometrisko un uzvedības atpazīšanu; sociālajai novērtēšanai ar mākslīgā intelekta palīdzību; slēptām mākslīgā intelekta sistēmām un dziļviltojumu tehnoloģijām (*deep fakes* – angļu val.); cilvēka un mākslīgā intelekta saskarnēm (*human-AI interfaces* – angļu val.).[668]

2020. gada decembrī Eiropas Padomes publicētajā CAHAI priekšizpētes ziņojumā tāpat ir norādīts, ka starptautiska nolīguma izveide par apšaubāma mākslīgā intelekta izmantošanu un sarkanajām līnijām var būt būtiska. Lietojumprogrammas, uz kurām varētu attiecināt sarkanās līnijas, ir, piemēram: attālinātas biometriskās atpazīšanas sistēmas vai citas uz mākslīgo intelektu balstītas novērošanas lietojumprogrammas, kas var izraisīt masveida novērošanu vai sociālo vērtēšanu; mākslīgā intelekta izmantošana slēptai manipulācijai ar personām. Katrs no šiem veidiem būtiski ietekmē personas autonomiju, kā arī demokrātijas pamatprincipus un brīvības. Šādu tehnoloģiju izmantošana, piemēram, valsts drošības mērķiem, būtu īpaši jāparedz ar likumu, tai ir jābūt nepieciešamai demokrātiskā sabiedrībā un proporcionālai likumīgam mērķim, un pieļaujamai tikai kontrolētā vidē un ierobežotu laika periodu.[669]

Eiropas Padomes sejas atpazīšanas vadlīnijās ir vērsta uzmanība, ka biometrisko datu apstrāde ar sejas atpazīšanas tehnoloģiju identifikācijas nolūkā būtu jāatļauj tikai saistībā ar tiesībaizsardzības mērķiem, ievērojot stingras nepieciešamības un samērīguma principus. Vadlīnijās valstu likumdevēji tiek mudināti pieņemt speciālus noteikumus attiecībā uz sejas atpazīšanas tehnoloģiju biometrisko apstrādi, citiem mērķiem nosakot precīzus izmantošanas pamatus, kā arī tajās vērsta uzmanība, ka privātie uzņēmumi nedrīkst izmantot sejas atpazīšanas tehnoloģijas nekontrolētā vidē, piemēram, iepirkšanās centros. Vienlaikus minētās vadlīnijas nenosaka skaidrus ierobežojumus vai pagaidu aizlieguma

668 Council of Europe, CAHAI Secretariat (2020), Towards regulation of AI systems; sk. arī Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence.

669 Council of Europe, CAHAI (2020), Feasibility Study.

piemērošanu attiecībā uz sejas atpazīšanas tehnoloģiju izmantošanu, ko veic tiesībaizsardzības vai citas valsts iestādes.[670]

Eiropas Savienībā arī ir vērsta uzmanība uz nepieciešamību noteikt sarkanās līnijas mākslīgā intelekta sistēmu izmantošanai. 2020. gada jūnijā Eiropas Parlamenta Pilsoņu brīvību, tieslietu un iekšlietu komiteja (LIBE) publicēja viedokli, kurā aicināja Eiropas Komisiju novērtēt pagaidu aizlieguma sekas sejas atpazīšanas sistēmu izmantošanā un atkarībā no šāda novērtējuma rezultātiem apsvērt pagaidu aizliegumu šo sistēmu izmantošanai valsts iestādēm publiskās vietās, izglītībā un veselības aprūpē, kā arī tiesībaizsardzības iestādēm daļēji publiskās vietās, piemēram, lidostās, līdz tehniskos standartus varēs uzskatīt par pilnībā atbilstošiem pamattiesībām, iegūtie rezultāti būs bez aizspriedumiem un nediskriminējoši un pastāvēs stingri drošības pasākumi pret ļaunprātīgu izmantošanu, un tie nodrošinās šādu tehnoloģiju izmantošanas nepieciešamību un proporcionalitāti.[671]

Eiropas Parlamenta 2020. gada 20. oktobrī mākslīgā intelekta tiesiskā regulējuma priekšlikumā netika noteiktas skaidras sarkanās līnijas. Tas neparedzēja aizliegumu mākslīgā intelekta masveida novērošanas tehnoloģiju izmantošanai, bet pamatā balstījās uz riska novērtējumu, nosakot pienākumus attiecībā uz augsta riska tehnoloģijām. Vienlaikus Eiropas Parlamenta rezolūcijā tiek uzsvērts: "Kaut gan mākslīgā intelekta, robotikas un saistīto tehnoloģiju ieviešanai publiskā sektora lēmumu pieņemšanā ir savas priekšrocības, no tās var rasties nepareizas lietošanas prakse ar smagām sekām, piemēram, masveida novērošana, prognozēšana tiesībaizsardzības nolūkā un attiecīgu procesuālo tiesību pārkāpumi."[672] Tātad masveida novērošana un prognozēšana tiesībaizsardzības nolūkā tiek uzskatīta par mākslīgā intelekta izmantošanu, kas rada "smagas sekas". Tāpat Eiropas Parlaments vērš uzmanību, ka pret tehnoloģijām, ko var izmantot automatizētu lēmumu pieņemšanai, tādējādi aizstājot publisko iestāžu pieņemtus lēmumus, ir jāizturas ar vislielāko piesardzību, it īpaši tiesas spriešanā un tiesībaizsardzībā. Dalībvalstīm šādas tehnoloģijas būtu jāizmanto tikai tad, ja ir pārliecinoši pierādījumi par to uzticamību un gadījumos, kad var tikt apdraudētas pamatbrīvības, ir iespējama vai sistemātiski tiek veikta jēgpilna cilvēka iejaukšanās un pārskatīšana. Tiek uzsvērts, ka svarīgi ir, lai valsts iestādes šajos gadījumos veic rūpīgu mākslīgā intelekta sistēmu pamattiesību ietekmes novērtējumu,

670 Council of Europe (2021), .. Convention 108.

671 European Parliament. Committee on Civil Liberties, Justice and Home Affairs (LIBE). (2020). Draft Report on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)), LIBE, Rapporteur Tudor Ciuhodaru. https://www.europarl.europa.eu/doceo/document/LIBE-PR-652625_EN.pdf

672 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

it īpaši tad, ja tās rada augstu risku. Ietekmes novērtējums kā atsevišķs mehānisms apskatīts nodaļas turpinājumā.[673]

Eiropas Komisijas MI akta priekšlikums savukārt paredz vairākas sarkanās līnijas. Aizliegumi ietver praksi, kurai var būt ievērojams potenciāls manipulēt ar personām, izmantojot subliminālus paņēmienus, personām to neapzinoties, vai izmantojot kādu neaizsargātu grupu, piemēram, bērnu vai invalīdu, ietekmējamību ar mērķi būtiski iespaidot viņu uzvedību veidā, kas var nodarīt fizisku vai psiholoģisku kaitējumu viņiem vai kādai citai personai. Priekšlikums arī aizliedz uz mākslīgo intelektu balstītu sociālo novērtēšanu, ko vispārējiem mērķiem veic publiskā sektora iestādes. Visbeidzot, aizliegta ir arī reāllaika biometriskās tālidentifikācijas sistēmu izmantošana sabiedriskās vietās tiesībaizsardzības nolūkos, ja vien nav piemērojami kādi ierobežoti izņēmumi.[674] Kā minēts ceturtajā nodaļā, minētajiem noteikumiem tika veltīta plaša kritika. Eiropas Datu aizsardzības uzraudzītājs un Eiropas Datu aizsardzības kolēģija kopīgajā viedoklī vērš uzmanību, ka sarkanās līnijas būtu jānosaka daudz stingrāk, un aicina vispārīgi aizliegt mākslīgā intelekta izmantošanu, lai automātiski noteiktu cilvēka pazīmes sabiedriskās vietās, piemēram, ne tikai no sejas attēla, bet arī no gaitas, pirkstu nospiedumiem, DNS, balss un citiem biometriskiem vai uzvedības signāliem jebkurā kontekstā. Minētās iestādes arī iesaka aizliegt kategorizēt personas, izmantojot biometriskos datus, pēc etniskās piederības, dzimuma, kā arī politiskās vai seksuālās orientācijas vai citiem diskriminācijas pamatiem. Tās vērš uzmanību, ka mākslīgā intelekta izmantošana fiziskas personas emociju uztveršanai ir ļoti nevēlama un tā būtu jāaizliedz. Iestādes arī norāda, ka būtu aizliedzamas mākslīgā intelekta sistēmas, kas nosaka vai klasificē personas turpmāko uzvedību, ņemot vērā, ka tās aizskar cilvēka cieņas būtību. Proti, tiesībaizsardzības iestādēm būtu aizliedzams izmantot mākslīgā intelekta sistēmas, lai veiktu individuālus riska novērtējumus, kuros vērtē: risku, ka fiziska persona izdarīs pārkāpumu vai atkārtotu pārkāpumu, vai risku, kam pakļauti iespējamie noziedzīgos nodarījumos cietušie. Tāpat būtu aizliedzamas mākslīgā intelekta sistēmas, ko paredzēts izmantot izdarīta vai paredzama noziedzīga nodarījuma izdarīšanas vai tā atkārtošanas prognozēšanai, pamatojoties uz fizisku personu profilēšanu, vai fizisku personu vai grupu personības un rakstura īpašību vai agrākas noziedzīgas rīcības novērtēšanai.[675]

Kā tika atklāts pirmajā nodaļā, vairākas ASV pilsētas ir jau noteikušas sarkanās līnijas sejas atpazīšanas tehnoloģiju izmantošanai tiesībaizsardzības iestādēs. Līdzīgi kā ES, arī ASV vairāk nekā 40 pilsoniskās sabiedrības organizācijas vēstulē

673 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

674 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

675 EDPB, EDPS (2021), EDPB-EDPS Joint Opinion 5/2021 ..

ASV prezidentam Džo Baidenam (*Joseph Robinette Biden*) aicina federālā līmenī steidzami noteikt pagaidu aizliegumu sejas atpazīšanas tehnoloģiju izmantošanai.[676] 2020. gada 2. decembrī Eiropas Komisija ierosināja jaunu ES un ASV globālo pārmaiņu programmu, kas aptver plašu tēmu loku, kurā tā aicina sākt kopā rīkoties attiecībā uz mākslīgo intelektu – balstoties uz kopīgo pārliecību par pieeju, kas būtu orientēta uz cilvēkiem, un risinot tādus jautājumus kā sejas atpazīšana –, kā arī vērš uzmanību, ka ES ierosinās sākt darbu pie transatlantiskā mākslīgā intelekta nolīguma, lai izveidotu vērtībām atbilstošu reģionālo un globālo standartu plānu.[677]

Starptautiskā, Eiropas, kā arī nacionālā līmenī būtu svarīgi stingri iestāties par cilvēktiesību ievērošanu un noteikt skaidras sarkanās līnijas. Būtu jāaizliedz mākslīgā intelekta novērošanas tehnoloģiju, it īpaši sejas atpazīšanas tehnoloģiju, izmantošana masveida novērošanai. Tiesiskajā regulējumā būtu jāparedz pagaidu aizliegums tiesībaizsardzības iestādēm izmantot sejas atpazīšanas tehnoloģijas, cita starpā mērķtiecīgai novērošanai, kamēr nepastāv skaidri pierādījumi par to efektivitāti, nav pieņemts atbilstošs regulējums, nosakot to ierobežojumus un aizsardzības pasākumus, un izstrādāti noteikti kritēriji, pēc kuriem var izvērtēt to darbības likumību un atbilstību cilvēktiesību prasībām. Būtu jāaizliedz arī personu emociju uztveršanas sistēmu, kā arī biometriskās kategorizācijas sistēmu izmantošana, ņemot vērā, ka šādi mākslīgā intelekta prakses veidi pārkāpj cilvēka cieņas un autonomijas principus. Līdzīgi cilvēka cieņa tiek aizskarta, izmantojot mākslīgā intelekta sistēmas prognozēšanai tiesībaizsardzības nolūkos, kā arī migrācijas, patvēruma, robežkontroles pārvaldībā, lai noteiktu un klasificētu personas uzvedību, izmantojot personu profilēšanu vai personības un rakstura īpašību novērtēšanu. Būtu jāaizliedz arī mākslīgā intelekta sistēmu izmantošana sociālai novērtēšanai un manipulēšanai ar iedzīvotāju uzvedību. Minētie mākslīgā intelekta izmantošanas veidi rada būtisku apdraudējumu un pārkāpj cilvēka cieņu, privātumu un citas cilvēktiesības, kā arī ir pretrunā ar demokrātiskām vērtībām.

Svarīgi ir nepalaist garām izšķirošu brīdi, kad tiek aktīvi lemts par mākslīgā intelekta tiesiskā regulējuma izstrādi un kad pastāv iespēja skaidri noteikt, tostarp Eiropas Padomes un ES līmenī, vai mākslīgā intelekta sistēmu konkrēta izmantošana, kas būtiski apdraud cilvēktiesības, ir pieļaujama vai nē. Runa pat nav par to, vai mēs varētu atbalstīt konkrēto izmantošanu vai nē. Skaidri ierobežojumi,

676 Coalition Letter Requests Federal Moratorium on the Use of Facial Recognition Technology. (16 February, 2021). *Freedom House.* https://freedomhouse.org/article/coalition-letter-requests-federal-moratorium-use-facial-recognition-technology

677 European Commission. (2020). Joint Communication to the European Parliament, the European Council and the Council. A new EU-US agenda for global change. https://ec.europa.eu/info/sites/default/files/joint-communication-eu-us-agenda_en.pdf

izmantošanas aizliegumi vai pagaidu aizliegumi nemaz nav jaunu sarkano līniju noteikšana, bet jau pastāvošo atzīšana. Proti, ir jāatzīst, ka mākslīgā intelekta tehnoloģiju izmantošana masveida novērošanai jau tagad nav savietojama ar cilvēktiesībām, tiesiskumu un demokrātijas principiem.

7.5. Ietekmes novērtējums

Ietekmes novērtējums ir viens no galvenajiem mehānismiem, kura nepieciešamība ir uzsvērta gan Eiropas, gan starptautiskajos mākslīgā intelekta regulējuma priekšlikumos.[678] Līdzās ietekmei uz cilvēktiesībām mākslīgā intelekta tehnoloģijas var radīt arī plašākus riskus, kas arī būtu jāņem vērā, veicot izvērtējumu.

Alesandro Mantelero piedāvā mākslīgā intelekta cilvēktiesību, sociālās un ētiskās ietekmes novērtējuma ideju. Viņš ierosina papildus cilvēktiesībām ņemt vērā arī ētisko un sociālo ietekmi.[679]

UNESCO Rekomendācijā par mākslīgā intelekta ētiku kā būtiskākais instruments ir norādīts ētiskās ietekmes novērtējums, kas ir norādīta kā pirmā no vienpadsmit politikas darbības jomām.[680] Dalībvalstis tiek aicinātas ieviest šādu novērtējumu, kas ļautu izvērtēt mākslīgā intelekta sistēmu ieguvumus un riskus, kā arī šo risku novēršanas, samazināšanas un uzraudzības pasākumus. Rekomendācija uzsver, ka ir nepieciešams novērtēt mākslīgā intelekta plašāku ietekmi uz cilvēktiesībām un pamatbrīvībām, darba tiesībām, vidi un ekosistēmu, kā arī ētisko un sociālo ietekmi.

Eiropas Padome arī iesaka izmantot cilvēktiesību ietekmes novērtējumu un rekomendē dalībvalstīm izveidot tiesisko regulējumu, kas nosaka valsts iestāžu procedūru, lai veiktu šādu novērtējumu mākslīgā intelekta sistēmām, ko šīs iestādes iegūst, izstrādā vai izmanto. Cilvēktiesību ietekmes novērtējums būtu jāievieš un jāīsteno līdzīgi kā citi ietekmes novērtējumu veidi, ko veic valsts iestādes, piemēram, novērtējums par ietekmi uz datu aizsardzību.[681] Savukārt CAHAI priekšizpētes ziņojumā ir norādīts, ka Eiropas Padomes līmenī varētu tikt izstrādāta vienota metodika un norādījumi cilvēktiesību, demokrātijas un tiesiskuma

678 ANO Uzņēmējdarbības un cilvēktiesību pamatprincipos uzņēmumiem ir paredzēta cilvēktiesību atbilstības pārbaude – prasība ievērot cilvēktiesības, paredzot, ka uzņēmumiem jāidentificē, jānovērš, jāmazina un jāatskaitās par negatīvo ietekmi uz cilvēktiesībām, ko rada viņu darbība. Sk. OHCHR (2011), Guiding Principles on Business and Human Rights.

679 Mantelero, A. (2018). AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment. *Computer Law & Security Review*, 34(4), pp. 754–772. https://doi.org/10.1016/j.clsr.2018.05.017

680 UNESCO (2021), Recommendation on the Ethics of Artificial Intelligence.

681 Council of Europe Commissioner for Human Rights (2019), Unboxing Artificial Intelligence ..

ietekmes novērtējumam vai integrētajam ietekmes novērtējumam, ko varētu izmantot, lai apliecinātu atbilstību principiem, kas tiks noteikti nākotnes Eiropas Padomes tiesiskajā regulējumā.[682] Būtiski ir izvērtēt ietekmi ne tikai uz cilvēktiesībām, bet arī plašāku ietekmi uz tiesiskumu un demokrātiju.

Pēdējo gadu laikā ir izteikti daudzi priekšlikumi ieviest algoritmisko ietekmes novērtējumu (*algorithmic impact assessments* – angļu val.). Piemēram, *AI Now* institūts mudina veikt algoritmisko ietekmes novērtējumu ikvienai valsts iestādei, ne tikai policijai, pirms tā plāno izmantot automatizētu lēmumu pieņemšanas sistēmu.[683] Kanāda ir izstrādājusi algoritmisko ietekmes novērtējumu saskaņā ar Kanādas Direktīvu par automatizētu lēmumu pieņemšanu, ko var piemērot dažādos gadījumos.[684] Eiropas valstis izstrādā mākslīgā intelekta atbildības rīkus, galvenokārt pamatojoties uz esošajiem datu aizsardzības noteikumiem. 2020. gada februārī Apvienotās Karalistes datu aizsardzības iestāde ICO publicēja vadlīniju projektu par mākslīgā intelekta audita sistēmu.[685] Šiem novērtējumiem par paraugu noder esošie ietekmes novērtējumi, piemēram, ietekmes uz privātumu novērtējums, ētikas ietekmes novērtējums, vides ietekmes novērtējums un it īpaši VDAR paredzētais novērtējums par ietekmi uz datu aizsardzību.[686] Pamatā tie mēģina skaidrot, kā piemērot datu aizsardzības normas attiecībā uz mākslīgā intelekta sistēmām un sniegt ieteikumus organizatoriskiem un tehniskiem pasākumiem, lai mazinātu mākslīgā intelekta radītos riskus personām.

ES izstrādātie mākslīgā intelekta tiesiskā regulējuma priekšlikumi arī ir pamatā balstīti uz riska izvērtējumu, paredzot pienākumus attiecībā uz augsta riska tehnoloģijām. Eiropas Komisija 2020. gada Baltajā grāmatā norāda, ka, izstrādājot jauno regulējumu, tā vēlas piemērot uz risku balstīto pieeju. Ņemot vērā augsto risku, ko daži mākslīgā intelekta izmantošanas veidi rada iedzīvotājiem un mūsu sabiedrībai, būtu nepieciešams objektīvs, iepriekšējs atbilstības novērtējums, lai pārbaudītu un nodrošinātu, ka tiek ievērotas noteiktas obligātās prasības. Atbilstības iepriekšējā izvērtēšanā varētu iekļaut testēšanas, apskates vai sertifikācijas procedūras. Tā varētu ietvert izstrādes posmā izmantoto algoritmu un datu kopu pārbaudes.[687]

682 Council of Europe, CAHAI (2020), Feasibility Study.

683 Sk. Reisman et al. (2018). Algorithmic Impact Assessments Report: A Practical Framework for Public Agency Accountability. AI Now Institute. https://ainowinstitute.org/publication/algorithmic-impact-assessments-report-2

684 Government of Canada. Algorithmic Impact Assessment. https://canada-ca.github.io/aia-eia-js/

685 Kazim, E., Denny, D. M. T., Koshiyama, A. (2021). AI Auditing and Impact Assessment: According to the UK Information Commissioner's Office. *AI and Ethics*, 1, pp. 301–310. https://doi.org/10.1007/s43681-021-00039-2

686 Sk. Reisman et al. (2018), Algorithmic Impact Assessments Report.

687 Eiropas Komisija (2020), Baltā grāmata par mākslīgo intelektu.

Eiropas Parlamenta rezolūcijā ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru attiecībā uz riska novērtēšanu ir norādīts, ka jebkurā nākotnes regulējumā būtu jāievēro diferencēta, uz risku balstīta un uz nākotni vērsta pieeja mākslīgā intelekta, robotikas un saistīto tehnoloģiju regulēšanai, tostarp piemērojot tehnoloģiski neitrālus standartus visās nozarēs, kā arī vajadzības gadījumā nozarei specifiskus standartus. Lai garantētu riska novērtēšanas sistēmas vienveidīgu īstenošanu un to, ka dažādās dalībvalstīs tiek nodrošināti vienlīdzīgi konkurences apstākļi un netiek pieļauta iekšējā tirgus sadrumstalošanās, ir vajadzīgs izsmeļošs un kumulatīvs augsta riska nozaru un augsta riska lietojuma veidu vai nolūku saraksts. Lai noteiktu, vai šīm tehnoloģijām piemīt augsts risks un līdz ar to attiecināma prasība ievērot mākslīgā intelekta tiesiskajā regulējumā paredzētos juridiskos pienākumus, visos gadījumos būtu jāveic objektīvs, reglamentēts un ārējs sākotnējās ietekmes (*ex-ante*) novērtējums, kas balstīts uz konkrētiem un definētiem kritērijiem. Par augsta riska tehnoloģijām būtu jāuzskata tāds mākslīgais intelekts, robotika un saistītās tehnoloģijas, kuru izstrāde, ieviešana un izmantošana var radīt būtisku kaitējuma risku konkrētām personām vai sabiedrībai kopumā, pārkāpjot ES tiesību aktos noteiktās pamattiesības un drošības noteikumus. Vērtējot to, vai mākslīgā intelekta tehnoloģijas rada šādu risku, būtu jāņem vērā nozare, kurā tās tiek izstrādātas, ieviestas vai izmantotas, to konkrētais lietojums vai nolūks un paredzamais kaitējuma smagums. Uz risku balstītā pieeja būtu jāizstrādā tā, lai ierobežotu administratīvo slogu uzņēmumiem, cik vien iespējams izmantojot jau esošus instrumentus, piemēram, VDAR paredzēto sarakstu attiecībā uz prasību veikt novērtējumu par ietekmi uz datu aizsardzību.[688]

Eiropas Komisijas MI akta priekšlikums ietver specifiskus noteikumus attiecībā uz mākslīgā intelekta sistēmām, kuras rada augstu risku fizisku personu veselībai un drošībai vai pamattiesībām. Attiecībā uz šīm sistēmām ir paredzēts ieviest riska pārvaldības sistēmu, lai novērtētu zināmus un paredzamus mākslīgā intelekta riskus, kā arī noteiktu to samazināšanas un uzraudzības pasākumus.

Augsta riska mākslīgā intelekta sistēmas ir atļautas Eiropas tirgū, ja ir nodrošināta atbilstība noteiktām obligātām prasībām un veikta atbilstības priekšnovērtēšana. Mākslīgā intelekta sistēmas, kuras paredzēts izmantot kā drošības sastāvdaļas produktos, ir pakļautas trešo personu atbilstības priekšnovērtēšanai. Savukārt attiecībā uz citām savrupām mākslīgā intelekta sistēmām, kurām galvenokārt ir ietekme uz pamattiesībām un kuras ir skaidri uzskaitītas III pielikumā, tiks izveidota jauna atbilstības un izpildes sistēma. MI akta priekšlikums paredz,

688 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

ka sagādātājs[689] pirms laišanas tirgū vai nodošanas ekspluatācijā veic sistēmas atbilstības novērtēšanu (19., 43. pants). Kā izņēmums ir paredzēts biometriskas tālidentifikācijas sistēmas, uz kurām attiektos trešās personas veikta atbilstības novērtēšana. Pēc attiecīgās atbilstības novērtēšanas pabeigšanas sagādātājam būtu jāreģistrē minētās savrupās augsta riska mākslīgā intelekta sistēmas ES datubāzē.[690]

Eiropas Datu aizsardzības uzraudzītājs un Eiropas Datu aizsardzības kolēģija publicētajā kopīgajā viedoklī norāda, ka būtu nepieciešams pielāgot priekšlikuma atbilstības novērtēšanas procedūru, lai trešās personas vienmēr veiktu augsta riska mākslīgā intelekta sistēmu *ex-ante* atbilstības novērtējumus. Turklāt tās vērš uzmanību, ka jebkurā mākslīgā intelekta sistēmas riska novērtējumā būtu jāņem vērā tehniskie parametri, kā arī tās īpašie lietošanas gadījumi un konteksts, kurā sistēma darbojas. Iestādes ierosina priekšlikumā norādīt, ka pakalpojumu sniedzējs veic sākotnējo sistēmas riska novērtējumu, ņemot vērā lietošanas gadījumus, un ka sistēmas lietotājs, kas darbojas kā datu pārzinis saskaņā ar ES datu aizsardzības tiesību aktiem, ja nepieciešams, veic datu aizsardzības ietekmes novērtējumu, ņemot vērā ne tikai tehniskos parametrus un lietošanas gadījumu, bet arī konkrēto kontekstu, kurā mākslīgā intelekta sistēma darbosies. Turklāt minētās iestādes iesaka precizēt MI akta priekšlikumu, piemēram, papildinot III pielikuma 1. punkta a) apakšpunktu, ietverot tajā mākslīgā intelekta biometrisko sistēmu izmantošanas gadījumus.[691]

Mākslīgā intelekta ietekmes novērtējumi var būt nozīmīgi atbildības rīki, kas nodrošina, ka iestādes un uzņēmumi apzinās un novērtē savu tehnoloģiju riskus, izvērtējot to plašāku ietekmi uz cilvēktiesībām, demokrātiju, sociālo, ētisko un cita veida ietekmi. Tie var būt arī efektīvs instruments, lai sabiedrību un indivīdus informētu par šādu sistēmu izmantošanu un sniegtu viņiem informāciju, kas var palīdzēt noteikt, vai šīs sistēmas ir atbilstošas. Tajā pašā laikā ES mākslīgais intelekts nebūtu jāregulē, pamatojoties uz risku, bet gan pamatojoties uz cilvēktiesībām.

Mākslīgā intelekta regulējums nedrīkstētu paredzēt, ka iestādes un uzņēmumi paši novērtē savas darbības riskus cilvēktiesībām, sabiedrībai, demokrātijai. Tas

689 MI akta priekšlikums paredz, ka "sagādātājs" ir fiziska vai juridiska persona, publiskā sektora iestāde, aģentūra vai cita struktūra, kura par samaksu vai par brīvu izstrādā vai liek izstrādāt AI sistēmu laišanai tirgū vai nodošanai ekspluatācijā ar savu vārdu vai preču zīmi (3. panta 2. punkts).

690 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

691 EDPB, EDPS (2021), EDPB-EDPS Joint Opinion 5/2021 ..

būtu fundamentāli nepareizs priekšstats par to, kas ir cilvēktiesības, jo cilvēktiesības nevar sabalansēt ar uzņēmumu interesēm.[692]

Uz risku balstīta pieeja mākslīgā intelekta regulējumam nav pietiekama, lai aizsargātu cilvēktiesības. Gan valsts iestādes, gan uzņēmumi var nebūt ieinteresēti mazināt riskus, lai izstrādātu, ieviestu un izmantotu tehnoloģijas. Kaut arī jau šobrīd ES datu aizsardzības regulējums uzliek pienākumu novērtēt mākslīgā intelekta novērošanas tehnoloģiju ietekmi uz personas tiesībām un brīvībām, kā apliecina daudzi prakses gadījumi, šis mehānisms efektīvi nenovērš tādu tehnoloģiju ieviešanu, kas pārkāpj datu aizsardzības prasības un personu tiesības.[693] Lai gan ES datu aizsardzības regulējums tieši neparedz ietekmes uz ES vērtībām, sabiedrību, tiesiskumu un demokrātiju izvērtējumu, sistēmas, kas rada kaitējumu šīm vērtībām, bieži vien pārkāpj arī personu tiesības un brīvības. Šis regulējums nosaka pienākumu novērtēt un novērst riskus personu tiesībām un brīvībām, tomēr praksē tas bieži vien netiek ievērots. Tāpēc uz risku balstīta pieeja mākslīgā intelekta regulējumam nav pietiekama, lai aizsargātu cilvēktiesības. Cilvēktiesības nav apspriežamas, un tās ir jāievēro neatkarīgi no riska līmeņa.

Neatkarīgai uzraudzības iestādei vajadzētu būt pilnvarām uzdot un uzraudzīt ietekmes novērtējuma veikšanu gan *ex-ante*, gan regulāri, kad sistēmas tiek izmantotas. Tas ir svarīgi divos gadījumos: ja pastāv draudi cilvēktiesībām un ja mākslīgā intelekta vai automatizēta lēmumu pieņemšanas sistēmas var būt neprognozējamas.[694]

Turklāt gadījumos, kad mākslīgā intelekta tehnoloģijas rada būtiskus vai neprognozējamus riskus cilvēktiesībām, sabiedrībai, demokrātijai, tiesiskumam un citām pamatvērtībām un esošajā tiesiskajā regulējumā nav piemērotu pasākumu, kas šos riskus novērstu, minētās tehnoloģijas būtu jāaizliedz vai jānosaka to pagaidu aizliegums, nosakot to tiesiskā regulējumā, nevis jāgaida, kad tas tiks paredzēts katrā konkrētajā gadījumā, kad tiek veikts ietekmes novērtējums. Attiecībā uz tādu augsta riska tehnoloģiju izmantošanu tiesībaizsardzības nolūkos kā sejas atpazīšanas tehnoloģijas un prognozējošās tehnoloģijas būtu jānosaka vispārējs aizliegums, atļaujot tās izmantot tikai izņēmuma gadījumos un paredzot efektīvus uzraudzības mehānismus, tostarp *ex-ante* izvērtēšanu, ko veic neatkarīga uzraudzības iestāde.

Būtu jāizveido efektīva pārvaldības sistēma, kas ietvertu tādas neatkarīgas uzraudzības iestādes izveidi, kura pilnvarota veikt vai pārraudzīt mākslīgā

692 Hidvegi, F., Leufer, D., Massé, E. (17 February, 2021). The EU should regulate AI on the basis of rights, not risks. *Access Now*. https://www.accessnow.org/eu-regulation-ai-risk-based-approach/

693 Sk., piemēram, EDPB (21 February, 2021), Swedish DPA ..

694 Hidvegi, Leufer, Massé (17 February, 2021), The EU should regulate AI ..

intelekta sistēmu novērtēšanu un īstenot efektīvus kontroles mehānismus. Turklāt būtu jāparedz arī plašas sabiedrības līdzdalības iespējas.

7.6. Neatkarīga uzraudzība, sabiedrības līdzdalība un atbildība

Lai nodrošinātu kontroli pār mākslīgā intelekta sistēmu izmantošanu, novērstu to radīto apdraudējumu cilvēktiesībām, tiesiskumam un demokrātijai, ir nepieciešams izveidot efektīvu, pārredzamu, sabiedrību iekļaujošu uzraudzības mehānismu.[695] Valstīm ir jāizveido kontroles mehānismi un jānodrošina efektīvi tiesiskās aizsardzības līdzekļi, lai nodrošinātu, ka mākslīgā intelekta attīstība un izmantošana atbilst tiesiskām prasībām.[696]

Eiropas līmenī ir izteikti daudzi priekšlikumi izveidot neatkarīgu uzraudzības iestādi, kas pārraudzītu, vai mākslīgā intelekta sistēmas darbojas, ievērojot cilvēktiesības un citas tiesiskās prasības. Eiropas Padomes cilvēktiesību komisārs 2019. gada rekomendācijā rosina valstis pieņemt tiesisko regulējumu, kas noteiktu neatkarīgu un efektīvu uzraudzības iestādi, kura pārraudzītu cilvēktiesību ievērošanu attiecībā uz mākslīgā intelekta sistēmu izstrādi, ieviešanu un izmantošanu, ko veic valsts iestādes un privātās organizācijas. Uzraudzības iestādēm ir jābūt neatkarīgām no valsts iestādēm un privātām organizācijām, kas izstrādā, ievieš vai citādi izmanto mākslīgā intelekta sistēmas, tām ir jābūt atbilstošai starpdisciplinārai kompetencei un resursiem, lai veiktu uzraudzības funkciju.[697] Rekomendācijā norādīts, ka šīm iestādēm būtu proaktīvi jāizmeklē un jāuzrauga mākslīgā intelekta sistēmu atbilstība cilvēktiesībām, jāsaņem un jārisina aizskarto personu sūdzības, kā arī periodiski vispārīgi jāpārskata mākslīgā intelekta sistēmu iespējas un tehnoloģiskā attīstība. Tām jāpiešķir pilnvaras iejaukties apstākļos, kad tās konstatē iespējamus cilvēktiesību pārkāpumus. Uzraudzības iestādēm būtu arī regulāri jāatskaitās parlamentam vai citām iestādēm un jāpublicē ziņojumi par savu darbību. Valsts iestādēm un privātiem uzņēmumiem pēc pieprasījuma vajadzētu sniegt informāciju, kas nepieciešama efektīvai mākslīgā intelekta sistēmu uzraudzībai, kā arī regulāri jāziņo uzraudzības iestādēm. Tām būtu jāīsteno uzraudzības iestāžu sniegtie ieteikumi attiecībā uz mākslīgā intelekta sistēmu ietekmi uz cilvēktiesībām. Uzraudzības procesam jābūt pārredzamam un pakļautam atbilstošai sabiedrības kontrolei. Uzraudzības iestāžu lēmumiem ir jābūt neatkarīgi pārvērtējamiem vai pārsūdzamiem.[698]

695 Council of Europe, CAHAI (2020), Feasibility Study.

696 Ibid.

697 Council of Europe Commissioner for Human Rights (2019), Unboxing Artificial Intelligence ..

698 Ibid.

Līdzīgi arī CAHAI priekšizpētes ziņojumā tiek uzsvērts, ka Eiropas Padomes dalībvalstīm vajadzētu noteikt un pilnvarot neatkarīgas struktūras, kas veiktu uzraudzību. Tās pārstāvētu un atskaitītos skaidri identificētai grupai ieinteresēto personu, kuras ietekmē mākslīgā intelekta praktiskā izmantošana. Tās varētu būt ekspertu komitejas, akadēmiskās vides pārstāvji, nozaru uzraudzības iestādes vai privātā sektora auditori. Tāpat valstis varētu apsvērt iespēju izveidot neatkarīgas uzraudzības iestādes, kurām būtu atbilstošas starpdisciplinārās zināšanas, pilnvaras un resursi to funkciju veikšanai. Ziņojumā norādīts, ka ir svarīgi atzīt arī esošo nacionālo cilvēktiesību, līdztiesības un ombuda institūciju nozīmīgo lomu, lai nodrošinātu efektīvu uzraudzību. Valstis varētu paplašināt esošo institūciju pilnvaras vai arī izveidot jaunas iestādes, kas izskatītu visas sūdzības, kā papildu mehānismu tiesību aizsardzībai tiesā. Tomēr nevar gaidīt, ka jebkura šāda struktūra varētu aptvert pilnīgi visus produktus un pakalpojumus, kas balstīti uz mākslīgo intelektu, un tāpēc būtu svarīgi ņemt vērā darbības jomu. Ja tiek izveidotas jaunas iestādes, to pilnvarām nevajadzētu pārklāties vai nonākt konfliktā ar iepriekš pastāvošo iestāžu pārraudzības funkcijām, kas aptver mākslīgā intelekta sistēmu īpašu izmantošanas veidu pārraudzību.

Ziņojumā vērsta uzmanība uz pienākumu valstīm uzraudzīt mākslīgā intelekta sistēmu izmantošanu publiskā sektora iestādēs. Mākslīgā intelekta sistēmu publiskajam iepirkumam būtu jāpiemēro atbilstoši uzraudzības mehānismi, nosakot juridiski saistošas prasības, kas nodrošina mākslīgā intelekta atbildīgu izmantošanu publiskajā sektorā. Daudzi publiskie dalībnieki mākslīgā intelekta sistēmas iegādājas no privātiem dalībniekiem un paļaujas uz tiem, lai iegūtu datus, ieviestu mākslīgā intelekta sistēmas un piekļūtu infrastruktūrai, kas ir pamatā un nodrošina mākslīgā intelekta sistēmas darbību. Privātajiem dalībniekiem ir pienākums nodrošināt, ka to sistēmas tiek izstrādātas un izmantotas atbilstoši prasībām. Uzraudzības iestādēm vajadzētu būt pilnvarām uzlikt privātajiem dalībniekiem pienākumu ievērot tiesiskās prasības mākslīgā intelekta kontekstā, it īpaši, ja pastāv risks, ka to intereses atšķiras no indivīdu un sabiedrības interesēm. Turklāt jānodrošina piekļuve tiesai, ja šie dalībnieki nepilda tiem uzliktos pienākumus.[699]

Arī ES līmenī ir vērsta uzmanība uz nepieciešamību izveidot neatkarīgu uzraudzības iestādi. Eiropas Parlamenta Regulas par mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrādes, ieviešanas un izmantošanas ētikas principiem priekšlikumā paredzēts, ka dalībvalstīm būtu jāizraugās neatkarīga administratīva iestāde, kas darbotos kā uzraudzības iestāde. Valsts uzraudzības iestādes palīdzētu nodrošināt regulas konsekventu piemērošanu visā ES, sadarbojoties gan savā starpā, gan ar ES iestādēm. Katra valsts uzraudzības iestāde darbotos kā

699 Council of Europe, CAHAI (2020), Feasibility Study.

pirmais kontaktpunkts gadījumos, kad rodas aizdomas par regulā noteikto ētikas principu un juridisko pienākumu pārkāpšanu, tostarp par diskriminējošu attieksmi vai citu tiesību pārkāpšanu, mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrādes, ieviešanas vai izmantošanas rezultātā. Šādos gadījumos attiecīgā valsts uzraudzības iestāde veic atbilstības novērtējumu, lai atbalstītu pilsoņu tiesības apstrīdēt un panākt savu tiesību aizsardzību. It īpaši uzraudzības iestādei vajadzētu būt atbildīgai par augsta riska mākslīgā intelekta tehnoloģiju apzināšanu un par šo tehnoloģiju atbilstības novērtēšanu un uzraudzību. Lai novērtētu un uzraudzītu augsta riska tehnoloģiju atbilstību, valsts uzraudzības iestādēm būtu jāsadarbojas arī ar citām iestādēm, kuras ir atbildīgas par reglamentējošu tiesību aktu nodrošināšanu saistītās nozarēs. Valsts uzraudzības iestādei būtu jānodrošina forums, kurā notiek regulāra viedokļu apmaiņa ar ieinteresētajām personām no akadēmiskajām aprindām, pētniecības vides, nozares un pilsoniskās sabiedrības un minēto personu starpā.[700]

ES MI akta priekšlikums paredz izveidot Eiropas Mākslīgā intelekta padomi, kurā piedalītos dalībvalstu un Eiropas Komisijas pārstāvji, kas veicinātu regulas netraucētu, efektīvu un saskaņotu īstenošanu, sekmējot valstu uzraudzības iestāžu un Eiropas Komisijas produktīvu sadarbību. Minētais priekšlikums paredz, ka valstu līmenī dalībvalstīm būs jānorīko viena vai vairākas valsts kompetentās iestādes, savukārt no to vidus – valsts uzraudzības iestāde regulas piemērošanas un īstenošanas uzraudzībai. Eiropas Datu aizsardzības uzraudzītājs savukārt darbosies kā kompetentā iestāde ES iestāžu, aģentūru un struktūru uzraudzībai.[701]

FRA norāda, ka ES ir labi attīstīts neatkarīgu institūciju kopums, kuru pilnvaras aizsargā un veicina pamattiesības, tās ir datu aizsardzības iestādes, līdztiesības organizācijas, valstu cilvēktiesību institūcijas un ombuda iestādes. FRA veiktais pētījums parāda, ka tie, kas izmanto vai plāno izmantot mākslīgo intelektu, bieži sazinās ar dažādām iestādēm par to izmantošanu, piemēram, datu aizsardzības iestādēm un patērētāju tiesību aizsardzības iestādēm.[702] Ne vienmēr var būt skaidrs, kura iestāde ir atbildīga par mākslīgā intelekta sistēmu uzraudzību. Visbiežāk mākslīgā intelekta izmantotāji sazinājušies ar datu aizsardzības iestādēm, lai iegūtu padomus, ieteikumus vai apstiprinājumu gadījumos, kad notiek personas datu apstrāde. Tomēr datu aizsardzības iestādēm šim uzdevumam nav pietiekamu resursu un tām trūkst īpašu zināšanu mākslīgā intelekta jautājumos. Ir jāpastiprina esošo uzraudzības iestāžu personāla zināšanas, lai tās varētu efektīvi uzraudzīt ar mākslīgo intelektu saistītos jautājumus, kas var būt izaicinājums.

700 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

701 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

702 FRA. (2020). Getting the future right. Artificial intelligence and fundamental rights. https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

Uzraudzības iestādēm ir jāpiešķir pietiekami resursi, pilnvaras un jānodrošina kompetence, lai novērstu un novērtētu pamattiesību pārkāpumus un efektīvi atbalstītu personas, kuru pamattiesības skar mākslīgais intelekts.

FRA uzsver arī sabiedrības līdzdalības nozīmi. Mākslīgā intelekta ietekmes uz cilvēktiesībām novērtējums varētu būt par pamatu konsultācijām ar dažādām ieinteresētajām personām un ekspertiem pirms konkrētās mākslīgā intelekta sistēmas izmantošanas. Apspriešanās ar attiecīgajām ieinteresētajām personām var nodrošināt, ka nepaliek nepamanīts iespējamais kaitējums un ka novērtējums tiek veikts no dažādām perspektīvām. Ieinteresētās puses varētu būt pilsoniskā sabiedrība, dažādas valsts un privātās organizācijas, kā arī cilvēktiesību un datu aizsardzības eksperti. Pilsoniskās sabiedrības organizācijām, kas specializējas tehnoloģiju, digitālo tiesību un algoritmu jomā, ir nozīmīga loma, lai veicinātu atbildīgu mākslīgā intelekta sistēmu izmantošanu. Efektīvai mākslīgā intelekta sistēmu uzraudzībai ir nepieciešama cieša sadarbība starp visām ieinteresētajām pusēm – valsts iestādēm, kurām jānodrošina pārraudzība, privātiem dalībniekiem, kuri var sniegt savas zināšanas un izstrādāt mākslīgā intelekta sistēmas, kas sniedz labumu sabiedrībai, kā arī pilsoniskās sabiedrības organizācijām, kas var pārstāvēt dažādu sabiedrības grupu intereses.[703]

A. Mantelero norāda, ka, ņemot vērā kolektīvo dimensiju, kāda ir datu izmantošanai mākslīgā intelekta sistēmās, cilvēku kontrole un uzraudzība nevar aprobežoties tikai ar uzraudzības iestādēm, datu apstrādātājiem vai datu subjektiem. Līdzdalības un demokrātiskas uzraudzības procedūrai būtu jādod balss sabiedrībai kopumā, tostarp dažādām cilvēku kategorijām, minoritātēm un nepietiekami pārstāvētām grupām. Arī ietekmes novērtējuma veikšanā būtu jāparedz sabiedrības līdzdalība. Būtu jāizstrādā riska novērtēšanas līdzdalības formas, aktīvi iesaistot iespējami skartās personas un grupas. Indivīdi, grupas un citas ieinteresētās personas būtu jāinformē un aktīvi jāiesaista debatēs par lomu, kādu mākslīgais intelekts ieņem sociālās dinamikas veidošanā un lēmumu pieņemšanas procesos, kas attiecīgās personas ietekmē. Atkāpes var paredzēt sabiedrības interesēs, ja tās ir proporcionālas demokrātiskā sabiedrībā un ja tiek nodrošinātas atbilstošas garantijas. Policijas, izlūkošanas un drošības jomā, kur sabiedrības uzraudzība ir ierobežota, valdībai ir regulāri jāziņo par mākslīgā intelekta izmantošanu.[704]

Aprakstītā neatkarīgā uzraudzība, kas paredz arī sabiedrības līdzdalību, ir tā sauktais stratēģiskais uzraudzības līmenis. Tam līdzās pastāv taktiskais uzraudzības līmenis, kas paredz noteikumus, kuri ir pieņemti attiecībā uz sistēmas izmantošanu noteiktos nolūkos un kuri paredz prasības, kādas ir jāievēro katrā

703 Council of Europe, CAHAI (2020), Feasibility Study.

704 Mantelero (2020), Regulating AI within the Human Rights Framework, p. 489.

konkrētajā gadījumā.[705] Novērošanas tehnoloģijām būtiska prasība ir iepriekšēja tiesneša akcepta jeb ordera saņemšana, kas ļauj veikt mērķtiecīgu novērošanu nacionālās drošības nolūkā, izmantojot, piemēram, sejas atpazīšanas tehnoloģijas. Šāda mehānisma izveidošana kā būtiska garantija pret negodprātīgu praksi un varas ļaunprātīgu izmantošanu izriet arī no ECT un EST prakses masveida novērošanas lietās, kas analizētas iepriekš grāmatas piektajā nodaļā.

Attiecībā uz taktisko uzraudzību sabiedrības līdzdalība ir stingri ierobežota. Bieži vien sabiedrība par to uzzina, kad persona iesniedz sūdzību uzraudzības iestādē vai tiesā vai, piemēram, ja tiek publicēta slēpta informācija, kā tas notika Snoudena atklājumu gadījumā. Vienlaikus arvien vairāk tiek pieprasīts, lai valsts iestādes informē sabiedrību par jauno tehnoloģiju izmantošanas praksi, īpaši tad, ja tās aizskar cilvēktiesības.

Neatkarīgas uzraudzības iestādes kontrole, kā arī visas sabiedrības pārraudzība ir sevišķi būtiska attiecībā uz augsta riska mākslīgā intelekta tehnoloģijām, kādas ir sejas atpazīšanas un citas masveida novērošanas tehnoloģijas. Ir nepieciešamas plašas debates, iesaistot ne tikai valsts iestādes, bet arī pilsonisko sabiedrību un zinātniekus, kurās būtu jārisina jautājumi gan par atbildības prasībām, kas piemērojamas mākslīgajam intelektam, gan plašāk par to, kādas ir biometriskās novērošanas un citu mākslīgā intelekta tehnoloģiju izmantošanas sarkanās līnijas. Uzraudzības un sabiedrības līdzdalības mehānismi kopā ļauj apturēt tādu tehnoloģiju ieviešanu un izstrādi, kas pārkāpj cilvēktiesības un demokrātijas principus, kā arī citas tiesiskās prasības. Par mākslīgā intelekta masveida novērošanas sistēmu atbilstību būtu jālemj nevis tikai policijai vai citām tiesībaizsardzības iestādēm, bet gan neatkarīgām uzraudzības iestādēm, iesaistot visu sabiedrību, un tām arī iepriekš jānovērtē, vai pastāv līdzsvars starp privātuma un drošības interesēm. Pilsoņu līdzdalībai ir būtiska loma, lai nodrošinātu lēmumu pārredzamību un atbildību, kā arī pasargātu personas no nelikumīgas novērošanas un atklātu prettiesisku praksi. Lai varētu efektīvi īstenot uzraudzību un sociālo līdzdalību, mākslīgā intelekta sistēmām ir jābūt arī pārredzamām.

7.7. Pārredzamība un informēšana

Mākslīgā intelekta sistēmu izmantošana bieži tiek slēpta vai nav zināma, tāpēc ir grūti vai neiespējami izvērtēt to ietekmi un uzraudzīt, vai tās tiek izmantotas tiesiski. Bez pārredzamības ir grūti noteikt, vai ir pārkāptas cilvēktiesības. Ja persona un sabiedrība kopumā nezina, ka to cilvēktiesības tiek aizskartas, tā nevar arī tās aizsargāt.

705 Schneier (2016), *Data and Goliath* .., pp. 189–190.

Sejas atpazīšanas un citas mākslīgā intelekta novērošanas tehnoloģijas bieži vien tiek izmantotas slepeni, arī Eiropā. Sabiedrībai ir maz zināms, kādas tehnoloģijas tiek izmantotas un kādā veidā, vai ir pierādījumi, ka tās tiešām ir vajadzīgas, un kas to apliecina. Šāda informācija ir jāatklāj gan uzraudzības iestādēm, gan sabiedrībai. Pārredzamības princips nodrošina cilvēka kontroli pār tehnoloģiju izmantošanu, lai mākslīgā intelekta sistēmas varētu pārbaudīt, saskaņot ar personu vēlmēm un ļautu personām, kuras šīs sistēmas ietekmē nelabvēlīgi, apstrīdēt to iznākumu.

Lēmumi, kas attiecas uz mākslīgā intelekta un citu jauno tehnoloģiju izmantošanas veidu, kuri var negatīvi ietekmēt cilvēktiesības un demokrātiju, kādas nepārprotami ir sejas atpazīšanas un cita veida novērošanas tehnoloģijas, nevar tikt pieņemti slepeni, bet gan par to ir jābūt atklātām diskusijām ar sabiedrību, sniedzot visu nepieciešamo informāciju, kas ļautu izvērtēt šo tehnoloģiju radīto ietekmi un to, vai šīm sistēmām var uzticēties. Ir vajadzīga plaša un stingra sabiedrības kontrole un visaugstākais iespējamais pārredzamības līmenis, kas sniegtu vispārēju pārskatu par mākslīgā intelekta tehnoloģiju izmantošanu tiesībaizsardzības jomā, kā arī ļautu veikt mākslīgā intelekta novērošanas tehnoloģiju risku novērtējumu.[706] Gatavojoties īstenot atbilstības, pārskatatbildības un kompensācijas pasākumus, vispirms ir jānodrošina mākslīgā intelekta sistēmu izmantošanas pārredzamība, jo tas var ietekmēt cilvēktiesības, demokrātiju un tiesiskumu.[707]

Pārredzamības prasības ir jānodrošina visas mākslīgā intelekta sistēmas uzraudzības laikā, un tas var ietvert gan pienākumu publiski izpaust informāciju par attiecīgo sistēmu, tās procesiem, tiešo un netiešo ietekmi uz cilvēktiesībām, gan par pasākumiem, kas veikti, lai identificētu un mazinātu sistēmas nelabvēlīgo ietekmi uz cilvēktiesībām. Pārredzamību var īstenot, arī veicot neatkarīgu, visaptverošu un efektīvu auditu. Visos gadījumos publiskotajai informācijai vajadzētu ļaut jēgpilni novērtēt mākslīgā intelekta sistēmu. Nevienai mākslīgā intelekta sistēmai nevajadzētu būt tik sarežģītai, lai tā nepieļautu cilvēku pārbaudi. Nedrīkstētu izmantot sistēmas, kas nevar nodrošināt atbilstošas pārredzamības un pārskatatbildības prasības.[708]

Tiesiskajā regulējumā būtu jāparedz skaidras pārredzamības prasības. Tas varētu ietvert tiesisku pienākumu publicēt mākslīgā intelekta sistēmu ietekmes novērtējumu, kā arī publisko konsultāciju atzinumu, kas atspoguļo ekspertu un sabiedrības pārstāvju paustos viedokļus, īpaši attiecībā uz augsta riska tehnoloģijām. Varētu tikt paredzēta prasība darīt pieejamu informāciju, kas ļautu

706 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

707 Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence.

708 Council of Europe Commissioner for Human Rights (2019), Unboxing Artificial Intelligence ..

uzraudzības iestādēm izvērtēt mākslīgā intelekta sistēmu atbilstību cilvēktiesībām, tiesiskumam un demokrātiskām vērtībām. Uzraudzības iestādei būtu arī jāizglīto un jāveicina sabiedrības izpratne par mākslīgā intelekta atbildības prasībām.

Viens no priekšlikumiem, kas būtiski veicinātu pārredzamību, ir mākslīgā intelekta sistēmu reģistra izveide. Dažādu policijas un citu tiesībaizsardzības iestāžu prakse var būt ļoti atšķirīga. Sejas atpazīšana tiek plaši izmantota dažādos kontekstos ar nelielu pārredzamību vai bez tās. Tāpēc būtu nepieciešams visu mākslīgā intelekta sistēmu vai automatizēto lēmumu pieņemšanas procesu reģistrs.[709] Valstīm vajadzētu izveidot sarakstu, kas ietvertu vismaz to mākslīgā intelekta tehnoloģiju izmantošanu, kas ir uzskatāmas par augsta riska tehnoloģijām saskaņā ar ES regulējumu. Reģistrā varētu tikt norādīta riska klase un nepieciešamais pārredzamības un atbildības apjoms konkrētai lietojumprogrammai.[710]

Reģistru varētu izveidot un uzturēt gan nacionālā līmenī, gan arī būtu atbalstāma ideja izveidot ES reģistru, kurā tiktu vienkopus atspoguļota informācija par visām ES dalībvalstīm. Lai uzlabotu publisko pārredzamību un pārraudzību un stiprinātu kompetento iestāžu veikto vēlāko uzraudzību, MI akta priekšlikums paredz ES līmenī izveidot augsta riska mākslīgā intelekta sistēmu datubāzi, kuru pārvaldīs Eiropas Komisija.[711]

Pārredzamība ir jānodrošina ne tikai mākslīgā intelekta sistēmu vispārējā uzraudzībā, bet arī attiecībā uz katru konkrēto mākslīgā intelekta izmantošanas gadījumu. Kā tika atklāts grāmatas iepriekšējā sestajā nodaļā, pārredzamības princips paredz, ka ikvienai personai ir tiesības būt pienācīgi informētai, kad viņa tieši mijiedarbojas ar mākslīgā intelekta sistēmu, saņemot viegli saprotamu un pieejamu informāciju par tās mērķi un sekām, tostarp par automatizētu lēmumu pieņemšanu. Mākslīgā intelekta sistēmas izmantošanai jābūt identificējamai jebkurā lēmumu pieņemšanas procesā, kas būtiski ietekmē personas cilvēktiesības. Katrai personai ir tiesības iesniegt pieprasījumu un uzzināt jebkura uz mākslīgo intelektu balstīta lēmuma pamatojumu, ja tāds ir pieņemts un attiecas uz šo personu.[712] Personām ir jāspēj saprast, kā tiek pieņemti lēmumi un kā šie lēmumi tiek pārbaudīti. Personām, attiecībā uz kurām valsts iestāde ir pieņēmusi lēmumu, tikai vai būtiski izmantojot mākslīgā intelekta sistēmas, vajadzētu par to paziņot un nekavējoties sniegt iepriekš minēto informāciju.[713]

709 Kayser-Bril (18 June, 2020), At least 11 police forces use face recognition ..

710 Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence.

711 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

712 Mantelero (2020), Regulating AI within the Human Rights Framework, p. 490.

713 Council of Europe Commissioner for Human Rights (2019), Unboxing Artificial Intelligence ..

Eiropas Padome vērš uzmanību, ka būtu aktīvi jāinformē personas un jāsekmē plaša sabiedrības izpratne par sejas atpazīšanas tehnoloģijām un to ietekmi uz pamattiesībām. Piemēram, sejas atpazīšanas tehnoloģiju integrēšana esošajās novērošanas sistēmās ne vienmēr paredz informēt tās personas vai sadarbības grupu pārstāvjus, kuru biometriskie dati tiek apstrādāti, piemēram, ja tiek apsvērta iespēja piekļūt personu digitālajiem attēliem internetā. Personām būtu vienkāršā veidā jāizskaidro tādi jēdzieni kā sensitīvie dati, biometriskie dati, kā darbojas sejas atpazīšana, kā arī jābrīdina par iespējamiem riskiem, kas var rasties neatļautas izmantošanas gadījumā. Likumdevējam un lēmumu pieņēmējiem būtu jāveicina sabiedrības iesaistīšanās sejas atpazīšanas tehnoloģiju izstrādes un izmantošanas uzraudzīšanā, kā arī piemērotu aizsardzības garantiju noteikšanā.[714]

Pārredzamība ir nepieciešama, lai radītu uzticēšanos mākslīgā intelekta sistēmām. Sabiedrības informēšana, kā arī plašas sabiedrības diskusijas var radīt šo uzticēšanos, kas ir pamats, lai sistēmas varētu ieviest, izmantot un lai sabiedrība tās pieņemtu, kā arī lai tās kalpotu sabiedrībai un tiktu novērsti to radītie riski.[715] Informētība un izglītotība ir būtisks nosacījums uzticama un uz cilvēku vērsta mākslīgā intelekta attīstībai. Sabiedrības izglītošana un izpratnes veidošana ir priekšnosacījums, lai personas apzinātos arī savu vērtību un tiesības un varētu tās aizsargāt.

7.8. Novērošanas tehnoloģiju uzraudzība pēc Covid-19 krīzes

Ir jārēķinās, ka pēc Covid-19 krīzes sabiedrība būs fundamentāli un neatgriezeniski pārveidota. Lai cīnītos ar pandēmiju, valstis visā pasaulē strauji sāka eksperimentēt ar digitālajām novērošanas tehnoloģijām. Grāmatas pirmajā nodaļā tika raksturotas dažāda veida tehnoloģijas, sākot no veselības lietotnēm, valkājamām aprocēm, kontaktu izsekošanas un citām mobilām lietotnēm, beidzot ar sejas atpazīšanas tehnoloģijām, ko valstis ieviesa ar mērķi nodrošināt sabiedrības veselību un drošību. Tāpat grāmatas iepriekšējās nodaļās[716] tika atklāts, ka šīs tehnoloģijas būtiski satricināja cilvēktiesības un lika pārvērtēt datu aizsardzības prasību piemērošanu. Šīs tehnoloģijas radīja daudz jaunu jautājumu par to, kā līdzsvarot privātumu ar sabiedrības drošības un veselības aizsardzības interesēm un pārredzamību, indivīdu intereses ar kolektīvajām interesēm, steidzamību ar

714 Council of Europe (2021), .. Convention 108.

715 Sk. OECD (2019), Recommendation of the Council on Artificial Intelligence.

716 Sk. grāmatas 1.2.5., 2.6., 3.6., 6.6. nodaļas.

pārdomātu rīcību. Tas, kā tiks atbildēts uz šiem jautājumiem, ilgtermiņā ietekmēs pilsoniskās brīvības, pārvaldību un tehnoloģiju lomu sabiedrībā.[717]

Valstīm būtu jāveido politika, kas nodrošinātu stingru uzraudzību pār šo tehnoloģiju ieviešanu un izmantošanu gan pandēmijas laikā, gan pēc tās. Krīze padarīja valdību lēmumu pieņemšanas procesu, tai skaitā jaunu tehnoloģiju un citu cilvēktiesību ierobežojošu pasākumu ieviešanu, daudz nedemokrātiskāku, slepenāku un nepārredzamāku. Šo tendenci var būt grūti apturēt. Grāmatas otrajā nodaļā tika pamatots, ka krīzes situācijā valstis nav atbrīvotas no cilvēktiesību ievērošanas. Līdzīgi krīze neatbrīvo valdības no prasības nodrošināt atbildīgu un demokrātisku jauno tehnoloģiju un citu pasākumu ieviešanu un uzraudzīt to turpmāku izmantošanu, nepieļaujot sarkano līniju pārkāpšanu. Iepriekš nodaļā aprakstītās garantijas – ietekmes izvērtēšanu, pārredzamību, informēšanu, neatkarīgu uzraudzību, sabiedrības līdzdalību – ir svarīgi ievērot, ieviešot jaunas tehnoloģijas arī krīzes situācijā. Tomēr daudzas no tehnoloģijām, to skaitā kontaktu izsekošanas lietotnes, tika ieviestas, nepastāvot skaidriem pierādījumiem par to efektivitāti vai pat standartiem, pēc kuriem izvērtēt efektivitāti. Skaidrs regulējums, kas paredzētu pienākumu ievērot minētās prasības, samazinātu iespēju, ka tās tiek ieviestas nepamatoti, neveicot to ietekmes izvērtējumu, kā arī novērstu to turpmāku izmantošanu pēc krīzes iepriekš neparedzētos nolūkos. Skaidrs regulējums, atbildības prasības un uzraudzības mehānismi ir būtiski ne tikai lai aizsargātu cilvēktiesības un demokrātiju, bet arī lai masveida novērošanas pasākumi nekļūtu par jauno normu.

Covid-19 krīze radīja ne tikai daudzus izaicinājumus, bet arī unikālu iespēju pārvērtēt tehnoloģiju ieviešanas un demokrātiskas pārvaldības politiku, procesus un sadarbības iespējas. Tā radīja daudzus pozitīvus piemērus efektīvai un ātrai valsts un privāto uzņēmumu sadarbībai ar mērķi sniegt kopīgu labumu sabiedrībai. Krīze liek domāt ārpus tradicionālās pieejas, veicinot starpdisciplināru, starpsektoru un starptautisko sadarbību. Tā liek pārdomāt attiecības starp digitālās suverenitātes aizsardzību un tehnoloģiju uzņēmumu datu vākšanu un analīzi.[718] Tā liek pievērst pastiprinātu uzmanību jautājumiem, kā nodrošināt gan valsts iestāžu, gan privāto uzņēmumu atbildību, piemēram, gadījumos, kad valsts sadarbojas ar tehnoloģiju uzņēmumiem, kas piedalās datu vākšanā un jauno tehnoloģiju nodrošināšanā, ņemot vērā, ka praksē lielā mērā tie nav pakļauti atbildības prasībām. Tā var likt izvērtēt jauno tehnoloģiju patiesās iespējas un tās nepārvērtēt. Krīze var likt pārdomāt arī jauno tehnoloģiju ietekmi uz cilvēktiesībām, to

717 Social Science Research Council. (2021). Surveillance and the 'New Normal' of Covid-19: Public Health, Data, and Justice. https://covid19research.ssrc.org/public-health-surveillance-and-human-rights-network/report/

718 Ibid.

ierobežošanu tādu sabiedrības interešu vārdā kā drošība un veselība. Principi un procesi, kas rodas šādas izvērtēšanas rezultātā, var atšķirties atkarībā no sabiedrībā pastāvošajām vērtībām. Ārkārtas apstākļi var arī veicināt mākslīgā intelekta uzticamību un atbildību, ieviešot mehānismus, kas iedzīvina praksē cilvēktiesības, tiesiskumu un demokrātijas principus.

Kopsavilkums

Mākslīgais intelekts rada jaunus apdraudējumus cilvēktiesībām, tiesiskumam un demokrātijai. Straujā mākslīgā intelekta attīstība ievērojami veicina novērošanas sabiedrības izveidi. Mākslīgā intelekta tehnoloģijas būtiski palielina varas nevienlīdzību gan no valsts, gan lielo tehnoloģiju uzņēmumu puses, ko vairs nedrīkst ignorēt. Arī pirms mākslīgā intelekta, kā to spilgti parāda Edvarda Snoudena atklājumi, valstis ir patvaļīgi izmantojušas tehnoloģijas un personas datus, lai slepeni veiktu masveida novērošanu, atsaucoties uz valsts un sabiedrības drošības aizsardzības interesēm, radot būtisku aizskārumu personu tiesībām uz privātumu, datu aizsardzību un citām cilvēka pamattiesībām. Kā liecina prakse, šādus pasākumus atcelt ir ļoti grūti, dažkārt pat neiespējami, un bieži vien tam ir nepieciešamas ilgstošas tiesvedības.

Mākslīgā intelekta novērošanas tehnoloģijas var radīt daudz ievērojamāku apdraudējumu. Gan Eiropā, gan citviet pasaulē valsts iestādes arvien plašāk ievieš sejas atpazīšanas, emociju uztveršanas un citas biometriskās sistēmas, kā arī prognozēšanas metodes tiesībaizsardzības nolūkos. Šīs sistēmas tiek izmantotas, lai veiktu masveida novērošanu, atsaucoties uz tādu būtisku sabiedrības interešu aizsardzību kā nacionālā drošība un sabiedriskā drošība. Arvien biežāk minētās sistēmas tiek izmantotas, lai izdarītu secinājumus un prognozes par cilvēku uzvedību, domām un citām personiskām īpašībām, kā arī, balstoties uz šīm prognozēm, tiek pieņemti lēmumi, kas var radīt personai nelabvēlīgas sekas. It īpaši autoritārās valstīs tās arvien vairāk izmanto sociālajai vērtēšanai, slēptai manipulācijai un cilvēku uzvedības kontrolei. Valstis vairs nevar ignorēt šādu mākslīgā intelekta tehnoloģiju izmantošanu, un būtu jāpieņem jauns juridiski saistošs regulējums, kas noteiktu stingrus ierobežojumus un aizliegtu tādas darbības, kuras ir pretrunā cilvēktiesībām, tiesiskumam un demokrātiskām pamatvērtībām.

Starptautiskās un Eiropas organizācijas plaši diskutē un meklē piemērotākos veidus, kā regulēt mākslīgo intelektu, un strauji izstrādā tiesisko regulējumu. Ir svarīgi nepalaist garām šo izšķirošo brīdi, kad starptautiskā un Eiropas līmenī ir iespējams noteikt skaidras sarkanās līnijas tāda mākslīgā intelekta izmantošanai, kas pārkāpj cilvēktiesības.

Regulējums, kas tiks pieņemts tuvākajos gados, noteiks turpmāko mākslīgā intelekta attīstību. Mēs atrodamies krustcelēs, kur ir iespējams izvēlēties, pa kuru no diviem ceļiem gribam iet. Vai vēlamies iet pa ceļu, pa kuru mūsu sejas attēlus fiksē sejas atpazīšanas tehnoloģijas, kas tos salīdzina ar plašām datubāzēm un analizē, vai mēs neesam izdarījuši vai neplānojam izdarīt noziedzīgu nodarījumu

vai likumpārkāpumu. Šo tehnoloģiju algoritmi daudz neprecīzāk darbojas attiecībā pret konkrētu grupu pārstāvjiem, veicinot diskrimināciju. Mūsu rīcības brīvība var tikt ierobežota, piemēram, izvēlē piedalīties pret valdību vērstās protesta akcijās, jo par to varam tikt sodīti, tāpēc ka tehnoloģijas ļaus identificēt protesta dalībniekus. Vai gribam, ka mūsu emocijas, jūtas, domas un uzvedību analizē mākslīgā intelekta algoritmi un ka, pamatojoties uz to rezultātiem, tiek pieņemti lēmumi, kas var radīt būtiskas sekas, piemēram, arestēšanu, pabalsta atteikšanu, atlaišanu no darba, neuzņemšanu augstskolā?

Vai arī mēs izvēlēsimies iet pa otru ceļu, kur mākslīgā intelekta sistēmas ir stingri regulētas, nosakot skaidrus ierobežojumus un sarkanās līnijas tādu tehnoloģiju izmantošanai, kas pārkāpj vai var būtiski aizskart cilvēktiesības, tiesiskumu un demokrātiju, kā arī skaidras aizsardzības garantijas, lai kontrolētu šo tehnoloģiju izmantošanu. Ejot pa šo ceļu, jau pirms tiek izstrādātas un ieviestas mākslīgā intelekta un citas jaunās tehnoloģijas, kas var radīt riskus un apdraudējumu cilvēktiesībām un pamatbrīvībām, ir jāpierāda to nepieciešamība, efektivitāte un samērīgums un neatkarīgai uzraudzības iestādei ir jāveic šo tehnoloģiju ietekmes novērtējums, iesaistot un uzklausot arī sabiedrības, nevalstisko organizāciju, dažādu grupu, kuras šīs tehnoloģijas var aizskart, pārstāvju un dažādu jomu ekspertu viedokļus. Novērtējumi visiem ir publiski pieejami. Tiek rūpīgi kontrolēts un uzraudzīts, vai esošās mākslīgā intelekta sistēmas tiek izmantotas atbildīgi un likumīgi, stingri ievērojot tiesiskā regulējuma prasības, tostarp datu aizsardzības noteikumus. Mākslīgā intelekta novērošanas tehnoloģiju izstrāde nenotiek slepeni, un tās netiek negaidīti ieviestas vai slepeni izmantotas, bet gan tiek publiskoti brīdinājumi, kas ikvienam sniedz saprotamu un skaidru informāciju par to izmantošanu. Mākslīgā intelekta sistēmu reģistrā var atrast informāciju par tādu mākslīgā intelekta sistēmu izmantošanu, kas var radīt augstu risku. Ir izveidoti mehānismi, lai personām, kuru tiesības un brīvības šo tehnoloģiju izmantošana apdraud, ir iespējams kolektīvi tās aizstāvēt un saņemt atbilstīgu atlīdzinājumu.

Šī izvēle netiek izdarīta vienā dienā. Mēs pastāvīgi veicam daudz dažādu izvēļu, turklāt krīzes situācijās var būt grūtāk izdarīt pareizās. Covid-19 pandēmija ievērojami pastiprināja masveida novērošanas tendenci. Visā pasaulē valstis strauji eksperimentēja ar dažādām digitālām tehnoloģijām, sākot no kontaktu izsekošanas lietotnēm, digitālajiem sertifikātiem, līdz pat valkājamām aprocēm, droniem un sejas atpazīšanas tehnoloģijām, lai kontrolētu iedzīvotāju pārvietošanos ar mērķi ierobežot vīrusa izplatību. Jāatceras, ka nekas nav tik paliekošs kā pagaidu pasākumi. Ir rūpīgi jāuzrauga jaunu tehnoloģiju un pasākumu, kas ierobežo cilvēktiesības, ieviešana un izmantošana, paredzot efektīvas aizsardzības garantijas, lai nepieļautu nesamērīgu cilvēktiesību ierobežošanu, kā arī lai masveida novērošana nekļūtu par jauno normu.

Tajā pašā laikā Covid-19 krīze radīja arī unikālu iespēju izvērtēt jauno tehnoloģiju nozīmi un kritiski skatīties uz to sniegtajām iespējām un efektivitāti. Tā lika pārvērtēt demokrātiskas pārvaldības politiku un procesus, cita starpā atklājot nepilnības attiecībā arī uz veidu, kādā valstī tiek ieviestas, izmantotas, izvērtētas un uzraudzītas jaunās tehnoloģijas. Tā atklāja arī to, cik ietekmīgs līdzeklis jaunās tehnoloģijas var kļūt valsts rokās, lai kontrolētu sabiedrību un ierobežotu cilvēktiesības, un kādus riskus un apdraudējumus tās var radīt.

Lai veicinātu uzticama, atbildīga un uz cilvēku vērsta mākslīgā intelekta attīstību, svarīga ir sabiedrības izglītošana un izpratnes veicināšana par mākslīgā intelekta tehnoloģijām, to radīto ietekmi, ieguvumiem un riskiem, kā arī par to ietekmi uz ētikas principiem un cilvēktiesībām. Tas ir priekšnoteikums turpmākai rīcībai, tai skaitā, lai tiktu pieņemts jauns mākslīgā intelekta regulējums, kas nosaka skaidrus ierobežojumus, aizsardzības garantijas un atbildības mehānismus, kas ir balstīti un aizsargā cilvēktiesības, tiesiskumu un demokrātiju.

Summary

The Role of Human Rights in the Age of Artificial Intelligence. Privacy, Data Protection and Regulation for Preventing Mass Surveillance

The monograph "The Role of Human Rights in the Age of Artificial Intelligence. Privacy, Data Protection and Regulation for Preventing Mass Surveillance" is the first scientific work in Latvia to analyse and explore the legal and human rights implications of artificial intelligence (AI).

AI is a technology undergoing rapid development and has become one of the most powerful drivers of social transformation. AI can bring great benefits in many areas, such as health care, education, culture, employment, transportation, environment, safety and national security and provide opportunities for economic, social, scientific and cultural development. At the same time, AI raises many challenges in all those areas as well as presenting serious ethical, legal and social issues. One of the most serious concerns is AI-based surveillance technologies that pose significant threats to human rights, the rule of law and democracy.

AI-driven surveillance technologies, such as facial recognition, emotional recognition and other biometric technologies, automated decision making and predictive analytics have been rapidly introduced in Europe and worldwide. A growing number of states is deploying AI technologies for surveillance purposes – facial recognition technology, smart city platforms, predictive policing, and automated border control systems, which are increasingly used by law enforcement authorities mainly for national security and public safety purposes. More than half of the world's advanced democracies employ artificial intelligence technologies.[719]

The use of facial recognition technology is growing rapidly worldwide both in public institutions and the private sector and it has come under the spotlight and faced major criticism. This technology is increasingly used by the police and other law enforcement authorities, often secretly and without control, a practice that is also present in many European countries, such as France, Germany, Spain, the Netherlands and the United Kingdom. It is also introduced by other public authorities and private companies to carry out surveillance at work, in schools, supermarkets, airports, sports events, and so on.

719 Feldstein, S. (2019). The Global Expansion of AI surveillance. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

International organisations, national legislators and supervisory authorities, non-governmental organizations, human rights defenders and academics are discussing how to regulate this technology and whether certain uses of AI surveillance technology should be prohibited. In 2019, San Francisco was the first US city to ban the use of facial recognition technology by government and law enforcement authorities, soon followed by Oakland, Boston, Minneapolis and other US cities.[720]

In Europe, an intense debate is ongoing about regulating and limiting the use of facial recognition technology. The Council of Europe has called for specific rules concerning biometric processing by facial recognition technologies for law enforcement purposes as well as to strictly limit or prohibit certain uses of these technologies.[721] The European Union (EU) considers regulation of facial recognition technologies as part of an initiative to create an ethical and legal framework for trustworthy AI. The European Commission's White Paper on Artificial Intelligence, published in 2020, emphasizes that the use and gathering of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks to human dignity, autonomy, the right to privacy and other fundamental rights.[722] On 21 April 2021, the European Commission proposed a new Regulation for Artificial Intelligence – known as the AI Act – that is the first initiative in the world that provides a legal framework for AI.[723] The new proposal acknowledges that some AI practices – including social scoring and the use of "real-time" remote biometric

720 Ravani, S. (17 July, 2019). Oakland bans use of facial recognition technology, citing bias concerns. *San Francisco Chronicle.* https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php; Lyons, K. (13 February, 2021) Minneapolis prohibits use of facial recognition software by its police department. *The Verge*. https://www.theverge.com/2021/2/13/22281523/minneapolis-prohibits-facial-recognition-software-police-privacy.

721 Council of Europe. (2021). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). Guidelines on Facial Recognition. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

722 European Commission. (2020). White Paper. On Artificial Intelligence – A European approach to excellence and trust. https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. See also European Parliament. (2020). Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies. https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html.

723 European Commission. (2021). Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

identification systems in publicly accessible spaces for law enforcement – should be prohibited, though at the same time this prohibition is subject to broad exceptions. These provisions have been criticised by the European Data Protection Supervisor and the European Data Protection Board, which have issued a joint statement calling for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces.[724]

Facial recognition technology is also attracting the attention of courts and national data protection authorities. The Swedish and French data protection authorities as well as a French court have issued decisions finding that use of facial recognition technology in schools violates the General Data Protection Regulation (the GDPR)[725].[726] The Swedish data protection authority has also found that the Swedish police authority has processed personal data in breach of data protection rules when using Clearview AI to identify individuals.[727]

The use of facial recognition technology and other forms of biometric mass surveillance in public places is increasingly opposed by civil society. In 2020, EDRi – the European network defending digital rights and freedoms – together with a wide range of civil society organisations launched the "Reclaim your face" campaign, accompanied by the European Citizens' Initiative in 2021, urging the European Commission to strictly regulate the use of biometric technologies and in particular to prohibit, in law and in practice, indiscriminate or arbitrarily-targeted uses of biometrics which can lead to unlawful mass surveillance in order to avoid undue interference with fundamental rights.[728]

724 EDPB, EDPS. (2021). EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en.

725 European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OV L* 119.

726 EDPB. (22 August, 2019). Facial recognition in school renders Sweden's first GDPR fine. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en; CNIL. (29 Octobre 2019). Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position. https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.

727 EDPB. (21 February, 2021). Swedish DPA: Police unlawfully used facial recognition app. https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_lv.

728 EDRi. (17 February, 2021). New ECI calls Europeans to stand together for a future free from harmful biometric mass surveillance. https://edri.org/our-work/new-eci-ban-biometric-mass-surveillance/. See also EDRi. (12 January, 2021). Re: Open letter: Civil society call for the introduction of red lines in the upcoming European Commission proposal on Artificial Intelligence. https://edri.org/wp-content/uploads/2021/01/EDRi-open-letter-AI-red-lines.pdf.

Besides facial recognition, other AI surveillance technologies, which analyse emotions and behaviour and are used for prediction and profiling, raise major concerns about their impact on human rights, democratic values and the rule of law.[729] As the global *biometrics* and emotional recognition market *grows,* there is a trend to use these technologies by law enforcement authorities across European countries lacking transparency, supervision and public involvement. The EU High-Level Expert Group on Artificial Intelligence (AI HLEG) has stressed that identifying and tracking individuals using biometric data, such as lie detection and personality assessment through micro expressions, and automatic voice detection, raises major AI-related concerns of both a legal and an ethical nature.[730] Another great concern is a growing reliance on AI-driven data analytics and predictive tools by police and law enforcement authorities in order to prevent and control crime.[731]

There has been a long and wide-ranging debate about the extent to which a state can use digital surveillance methods of data collection and analysis to carry out surveillance in order to protect such public interests as national security and public safety. Growing security threats have expanded mass surveillance practices all around the world. Edward Snowden's revelations on the US secret mass electronic surveillance program of global telecommunication and data flows of both US and other countries' citizens on a previously unimaginable scale introduced after the 9/11 terrorist attacks triggered global concerns about the impact on human rights of mass surveillance practice by intelligence and law enforcement agencies, in particular on the right to privacy and data protection, as well as lack of regulation, transparency and effective safeguards.[732]

Extensive mass surveillance measures in the name of national security have been introduced not only in the US but also in Europe at both EU and national levels. The European Court of Justice (the CJEU) and the European Court of Human Rights (the ECtHR) play a key role in limiting mass surveillance practices

729 See, e.g., Mcstay, A. (2020). Emotional AI, Soft Biometrics and The Surveillance of Emotional Life: An Unusual Consensus on Privacy, Big Data & Society.

730 AI HLEG. (2019). Ethics Guidelines for Trustworthy AI. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

731 See, e.g., McDaniel, J. L. M., Pease, K. G. (2021). Introduction. In: McDaniel, J. L. M., Pease, K. G. (eds.), *Predictive Policing and Artificial Intelligence*. Routledge, pp. 1–38; van Brakel, R. E. Rethinking predictive policing: Towards a holistic framework of democratic algorithmic surveillance. In: Schuilenburg, M. & Peeters, R. (eds.), *Algorithmic Societies: Power, Knowledge and Technology in the Age of Algorithms*. Routledge, pp. 104–118.

732 See, e.g., OHCHR. (2014). The right to privacy in the digital age, UN Doc. A/HRC/27/37.

as well as promoting and protecting compliance with the right to privacy, data protection and other human rights in the context of mass surveillance.[733]

As an urgent counter-terrorism measure in response to the terrorist attacks in Madrid in 2004 and in London in 2005, the EU Data Retention Directive[734] was swiftly adopted in 2006, despite many concerns about its non-compliance with fundamental rights. In 2014, the CJEU judgment in the *Digital Rights Ireland* case annulled the directive, recognizing that it constitutes an unjustified interference with fundamental rights by requiring EU Member States to oblige telecommunications and internet service providers to retain certain categories of non-content data and to make it available on request to law enforcement authorities for the purposes of investigation, detection and prosecution of serious crime and terrorism.[735] The CJEU has also adopted a number of judgments in response to US mass surveillance practice. It adopted two judgments – in 2015 in *Schrems* I[736], and in 2020 in *Schrems* II[737] – twice annulling European Commission decisions on the adequacy of the level of protection for data transfers from the EU to the US. The ECtHR has been resolving many cases about compliance of national mass surveillance measures with human rights, seeking to find a balance between a person's right to privacy and data protection, on the one hand, and national security and national security interests, on the other hand.[738] The extensive case-law of both courts shows that cancellation of mass surveillance measures introduced for security purposes at both EU and national levels is very difficult and often only possible after lengthy court proceedings.

Alongside the threat of terrorism and security, the Covid-19 crisis caused an even greater flood of new surveillance technologies. To combat the spread of the pandemic, countries around the world have rapidly introduced digital

733 See, e.g., Nesterova, I. (2019). Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards. In: *How International Law Works in Times of Crisis*. Ulrich, G., Ziemele, I. (eds.), Oxford University Press, pp. 109–125.

734 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105.

735 Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* ECLI:EU:C:2014:238.

736 Case C-362/14, *Maximillian Schrems v Data Protection Commissioner,* ECLI:EU:C:2015:650.

737 Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems,* ECLI:EU:C:2020:559

738 See, e.g., European Court of Human Rights. (2020). Guide on Article 8 of the Convention – Right to respect for private and family life. Available: https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

surveillance technologies, ranging from health apps, wearable bracelets, contact tracking and other mobile apps, and digital certificates, to drones and facial recognition technologies.[739] These experiments have significantly shaken human rights, raising new questions about the extent to which privacy, data protection and other human rights can be restricted to ensure public health and safety as well as ways to balance individual and collective interests. Exceptional circumstances do not cancel the requirement to respect human rights.

It is crucial to address the legal, ethical and social issues related to the use of AI and other surveillance technologies in a timely manner. These technologies have a new kind of impact on human rights; they significantly enhance public control based on goals and values that may contradict the values of a democratic society. China's social scoring and so-called 'social credit' system is the most dramatic example.[740]

AI surveillance technologies are different from previous forms of digital surveillance. AI offers new possibilities for data collection, processing and analysis, allows observation to be carried out on a much wider scale and in a more detailed and precise way, thus significantly facilitating the use of surveillance measures. Use of these technologies poses new types of specific risks. They pose a serious threat to the right to privacy and data protection, human dignity and non-discrimination, freedom of expression and peaceful assembly, and to other human rights and freedoms. Moreover, they have a wider impact on the rule of law and democracy.[741] AI significantly increases the scale of mass surveillance by the state and large technology companies and increases power inequalities. Shoshana Zuboff points out that surveillance capitalism has disastrous consequences for democracy and freedom, as it has amassed unprecedented concentrations of knowledge and power with hardly any interference from laws and regulations. This asymmetry of knowledge and power raises new forms of social inequality, and allows shaping of behaviour by individuals and populations in

739 Couch, D. L., Priscilla, R., and Komesaroff, P. A. (2020). COVID-19 – Extending Surveillance and the Panopticon. *Journal of Bioethical Inquiry.*

740 Carney, M. (17 September, 2018). Leave no dark corner. *ABC*. http://mobile.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278?pfmredir=sm&sf197878142=1&smid=Page:%20ABC%20Australia-Facebook_Organic&WT.tsrc=Facebook_Organic.

741 See, e.g., Council of Europe, CAHAI Secretariat. (2020). Towards regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law. https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a.

ways that are inherently antidemocratic.[742] Although this book focuses on state mass surveillance, with commercial surveillance beyond its scope, nevertheless the challenges posed by commercial surveillance, particularly the algorithms of social media platforms that influence and manipulate user opinion, social and political behaviour, are equally important and would deserve a separate study.

In order to ensure that the use of AI is in line with human rights and does not violate them, it is crucial to assess the existing regulatory framework as well as to develop new strong regulation setting clear limits on when AI can and cannot be used and requiring effective safeguards and supervision mechanisms. There is an urgent need to set limitations on AI surveillance measures in order to protect human rights and democratic values. Regulation is an essential tool in order to ensure accountable and human-centred AI, and to prevent the potential harm it can cause.

In the last few years, international organizations – notably the Council of Europe[743], the United Nations Educational, Scientific and Cultural Organization (UNESCO)[744], the Organization for Economic Co-operation and Development (OECD)[745], the EU[746], as well as many non-governmental, professional and other organizations[747] – have been rapidly developing ethical guidelines defining the values, principles for development, implementation and use of AI. However, there is a growing emphasis on the need for regulation to go beyond ethical

742 Naughton, J. (20 January 2019). 'The goal is to automate us': welcome to the age of surveillance capitalism. *The Guardian.* https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook. See also Zuboff, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the new Frontier of Power*. Profile Books.

743 Council of Europe. (2020). Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the human rights impacts of algorithmic systems. Adopted 08.04.2020. https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

744 UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137.

745 OECD. (2019). Recommendation of the Council on Artificial Intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

746 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

747 See, e.g., IEEE. (2019). Ethically Aligned Design. First Edition: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems. https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf?utm_medium=undefined&utm_source=undefined&utm_campaign=undefined&utm_content=undefined&utm_term=undefined; Fjeld, J., Achten, N., Hilligoss, H., et al. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Berkman Klein Center Research Publication No. 2020-1. https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y.

norms, and to establish legally binding requirements at both the international and national level, and to implement effective practical mechanisms to put AI ethical principles into practice. Both international organizations and countries around the globe are currently actively looking for possible ways to regulate AI.

At the same time, the existing legal framework – particularly human rights and data protection rules – are already applicable to AI. Human dignity, the right to privacy and data protection, the principle of non-discrimination, freedom of expression and assembly, and other human rights and freedoms are of particular importance and are applicable to AI surveillance technologies. These rights and freedoms can help to redefine red lines in terms of their use. The requirements on collection and use of personal data and accountability measures that are set in the data protection rules – particularly in the GDPR and the Law Enforcement Directive[748] – are also critical in relation to the development, deployment and use of AI surveillance technologies.

The book demonstrates that human rights and data protection standards provide the most secure basis for further development of AI regulation, and that a clear AI legal framework needs to be introduced by further developing international human rights and European data protection rules, building upon the existing case-law of the CJEU and the ECtHR. In addition, clear limitations need to be set on certain uses of AI surveillance technologies. It is therefore necessary to fully assess the effectiveness and shortcomings of the existing legal framework and then consider the need for a new framework. New legislation should only be adopted once the issue has been properly understood, following public debate, and once it has been established that existing laws are not sufficient to address the issues identified.

In this book, a coprehhensive approach is taken to to analyse and explore the legal and human rights implications of AI as well as surveillance technologies, their risks and threats, providing concrete recommendations for the development of regulation and policy at both international and national levels.

This book aims to examine the human rights implications of AI surveillance technologies and evaluate existing and future regulation in order to prevent the risks and threats posed by these technologies. More specifically, the author explores the development of AI mass surveillance technologies and their use by law enforcement authorities in Europe and beyond. The author proceeds to

748 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L* 119, 04.05.2016.

analyse the impact of these technologies on human rights as well as the wider effect on society and fundamental democratic principles. Further on, the author evaluates how the rights to privacy and data protection, the conditions for their limitations developed in case-law and European data protection standards apply to AI surveillance technologies, as well as examining AI regulation at both international and EU levels. Lastly, the research offers recommendations for development of a legal and regulatory framework for AI surveillance technologies and the safeguards and mechanisms that should be introduced to prevent threats and risks and ensure responsible and human-centric use of AI surveillance technologies.

Analysis of human rights, data protection and AI regulatory and legal framework, guidelines and other documents developed and adopted by the UN, UNESCO, the Council of Europe, the OECD and EU institutions, plays an important role in the study. Documents developed by national institutions and data protection institutions and other public institutions, non-governmental organizations, and international AI expert groups have also been used in the work. In addition, the book extensively analyses and compares the case-law of the ECtHR and the CJEU. Although the research mainly analyses legal aspects of AI surveillance technologies, the study makes extensive use of an interdisciplinary approach. In order to understand AI technologies and reveal not only their legal, but also their social and ethical implications as well as their impact on society and democracy, a wide range of research was examined: books, scientific articles, reports and other documents in sociology, ethics, philosophy, politics, technology and other fields.

The book is organized in seven chapters. This summary will briefly describe the topics examined in each chapter, the main conclusions, proposals and recommendations, which are mostly provided in the last two chapters, that is, in Chapter 6, where proposals for improving data protection rules are laid down and in Chapter 7, which summarises the analyses and offers policy recommendations for the further development of human rights-based AI.

Chapter 1, AI and state surveillance, introduces the topic and explains AI and surveillance from a social and technological point of view, revealing how the development of new technologies from big data to AI has influenced and facilitated mass surveillance. First of all, technological concepts are explained, that is, AI (definition and subdomains), the relation of AI to big data, personal data and the concept of profiling. It goes on to explain the concept of surveillance, the imbalance of power as a feature of surveillance, the distinction between mass surveillance and targeted surveillance as well as examining how national security and public safety have long been fertile ground for introducing various types of mass surveillance measures by law enforcement and intelligence agencies.

The chapter then explores how AI has significantly increased surveillance practices and examines specific AI surveillance technologies and methods – facial recognition technology, emotion recognition technology and predictive policing – and, finally, reveals how the Covid-19 crisis has contributed to the use of digital surveillance technologies.

Chapter 2 examines the impact of AI surveillance measures on human rights. The chapter examines human rights that are most impacted by those measures: – human dignity; – the right to privacy and data protection; – the principle of non-discrimination, – the rights of the child; – the rights to an effective remedy and to a fair trial; – freedom of expression; – freedom of assembly and association. The book examines how these rights are regulated in international and European human rights instruments, in particular the European Convention on Human Rights (the ECHR), the Charter of Fundamental Rights of the European Union (the Charter) and the Constitution of the Republic of Latvia[749], revealing how these rights are challenged by AI mass surveillance measures. The chapter goes on to explore the wider impact of these technologies on society, the rule of law and democratic values.

Human dignity constitutes the foundation of all human rights and fundamental freedoms and is essential for the development, deployment and use of AI systems. Every human being possesses an intrinsic value and should be treated with respect; this also applies with regard to use of AI systems. Human dignity should be the counterweight to mass surveillance practices and asymmetry of power. Likewise, AI surveillance practices touching the essence of the right to human dignity should be prohibited.

The right to privacy includes a wide range of elements. Besides personal or general privacy, it also encompasses physical, psychological or moral integrity, and the identity and autonomy of the person. AI surveillance technologies have a profound impact on all these elements. Use of facial recognition technology involves acquisition, comparison and storage of biometric facial images in IT systems. Each of these actions constitutes an interference with the right to privacy and the right to protection of personal data. Other forms of AI biometric recognition, which include analysing and predicting our behaviour and emotions through facial expressions, tone of voice, gait, and heart rate, further affect our psychological integrity, deeply interfere with our personal sphere and severely limit our ability to freely express our personality and autonomy. It is important to remember that very often no scientific evidence is available on the claimed abilities of AI technologies; for example, there is no proof that a person's inner

749 The Constitution of the Republic of Latvia. Adopted on 15. February 1922 (came into force on 7 November 1922). *Latvijas Vēstnesis*, 01.07.1993., No 43.

emotions can be accurately "read" from facial expressions, heart rate or tone of voice.

Use of AI surveillance systems can lead to discrimination. Studies have shown that AI algorithms in facial recognition technology work differently depending on the age, gender, or ethnicity of the person being identified. As a result, members of these groups may be more likely to be discriminated against, for instance more often being unwarrantedly stopped or detained by police. The use of such technologies could be used to control and track the most marginalized communities and enhance discrimination against certain ethnic groups. AI surveillance systems can have a particularly negative impact on vulnerable groups such as children and the elderly, especially as the accuracy of face recognition is significantly lower for children.

Children and their rights are significantly affected when they are directly engaged with AI surveillance activities, but also in the case of indirect engagement through tools such as surveillance cameras and predictive modelling. The well-being and full development of children are limited when their freedom and autonomy are constantly restricted by AI systems, including surveillance systems.[750]

AI surveillance technologies can also restrict individuals' right to a fair trial and effective remedies. Facial recognition systems often make mistakes in determining whether a person is dangerous. This, in turn, can lead to unjustified detention, accusation and even conviction of innocent people. The use of AI systems in law enforcement may raise concerns about fair trial standards, in particular the presumption of innocence, the right to be informed promptly of the cause and nature of accusation, the right to a fair trial and the right to defend oneself.

The use of surveillance measures such as facial recognition technology in public places may restrict a person's right to freely express their views and opinions, as well as freedom of assembly and association. Surveillance of public places with facial recognition technologies can have a chilling effect and can make people change their behaviour and impact their willingness to attend demonstrations or engage in public activism.

In addition to posing risks to human rights, AI surveillance technologies can also endanger the rule of law and democracy. The rights to freedom of expression, freedom of assembly and association are essential in a democratic society. The use of new technologies, which can disproportionately restrict and violate those freedoms, also threatens the very foundations of a democratic society.

750 UNICEF. (2020). Policy guidance on AI for children. Draft 1.0. https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf.

The chapter also examines the obligation to respect human rights during a crisis situation, stressing that even in such emergencies as Covid-19 citizens do not have to choose between respecting human rights and protecting such interests as public safety and health. Restrictions on human rights must still be legitimate, necessary and proportionate in terms of achieving the particular aim, as well as limited in time.

Chapter 3 analyses the importance of privacy. Mass surveillance exercises a significant impact on the right to privacy; moreover, many attempts are being made to devalue privacy – and are being widely criticized. The chapter reveals why privacy should be protected and outlines its value and meaning, before going on to examine various theories and analysing the rationale and role of the right to privacy in limiting AI mass surveillance measures. It reveals that the right to privacy has been recognized as: – the right to be left alone, – the right to control information about oneself; – an essential aspect of human dignity, autonomy and free will; – protection against abuse of power. The chapter looks at the right to privacy in international human rights treaties and explores how this right helps to protect other human rights, for example, freedom of expression and assembly. It also reveals how academics increasingly acknowledge the importance of group privacy, which protects against pervasive mass surveillance and asymmetry of power. Further, the importance of rising awareness about privacy has been highlighted, spearheaded by a number of individuals, in particular Edward Snowden, Maximilian Schrems as well as fostered through *Cambridge Analytica* and other scandalous cases of illegal use of data by large technology companies. The end of the chapter brings to attention the fact that the Covid-19 crisis can also lead to a crisis of privacy. There is an urgent need for a new regulatory framework to prevent threats to privacy and other human rights.

Chapter 4 contains an overview on the development of data protection law and the first initiatives to regulate AI. The chapter begins with a brief introduction on how data protection law marks the beginning of information and communication technology rules trying to balance the different public and private interests. After that, it introduces international initiatives and the EU path from the data protection golden standard to AI regulation.

Section 1 examines how international organisations – the Council of Europe, the OECD, the UN, UNESCO – have developed data protection law, how these organisations have engaged in the debate about the impact of mass surveillance on human rights as well as exploring their first actions towards creating AI regulation.

International organizations, especially the Council of Europe and the UN, have for a long time been calling for revision of international as well as national rules and for strengthening data protection standards in order to provide effective safeguards against mass digital surveillance measures. The recommendations

provided by those organisations are largely applicable to AI surveillance measures. Many earlier proposals regarding regulation of digital surveillance can be found in AI ethical guidelines, such as requirements to respect the principles of proportionality, transparency and accountability.

Section 2 examines the development of EU data protection law. Firstly, it is noted that the EU is founded on respect for human rights, freedom, democracy and the rule of law, and that the importance of human rights has greatly increased in EU legislation. The EU's fundamental rights-based approach, which underpins the development of data protection law, should also form the basis for the further development of AI regulation.

This is followed by an examination of EU data protection reform and the GDPR as well as specific legal instruments on data protection, especially the Law Enforcement Directive. The author draws attention to the fact that the EU data protection rules do not constitute a fully uniform system. Both the EU and Member States should review legal acts adopted before the GDPR and assess the necessity for new specific data protection rules, including in relation to AI application in different sectors. The data protection rules will be strongly influenced by the regulatory framework that is being developed for Europe's digital future, including AI regulation.

Finally, the author examines the development of AI regulation in the EU. To date, discussions on AI regulation are fundamentally based on the EU's digital single market agenda. While these policy discussions may refer to the need to consider law enforcement and criminal law specificities, they often lack detailed review and fail to take into account specific applicable rules, in particular restrictions and derogations.[751] The chapter reveals that both international organisations and the EU are rapidly developing new regulation, effective safeguards and accountability mechanisms for AI systems, including new provisions for preventing and limiting the use of AI surveillance technologies.

Chapter 5 analyses the jurisprudence of the CJEU and the ECtHR on interference with the right to privacy and data protection through mass surveillance.

Section 1 explains the conditions for limiting the right to privacy and other rights and freedoms set out in the ECHR and the Charter. Section 2 analyses the most important cases: the case-law of the ECtHR examining whether national surveillance measures comply with human rights as well as the case-law of

751 Gonzelez Fuster, G. (2020). Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf. See also Drechsler, L. (2021). Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context. *International Data Privacy Law*, 11(2), pp. 182–195. https://doi.org/10.1093/idpl/ipaa019

the CJEU on mass surveillance cases related to the validity or interpretation of EU law. Section 3 examines the four essential guarantees based on the jurisprudence of the CJEU and the ECHR:

- clear, precise and accessible rules;
- proportionality and necessity;
- independent oversight mechanism; and
- effective remedies.[752]

The case-law of both courts reveals that mass surveillance measures constitute an intrusion into privacy and data protection. It is essential to have clear, precise and accessible rules governing the scope and application of these measures. The rules should provide minimum safeguards against arbitrary interference and the risk of abuse that counterbalance secrecy and allow individuals to foresee when the authorities are likely to apply these measures, thus allowing them to adjust their behaviour.

On the principle of proportionality, the ECtHR and the CJEU have emphasized that one of the crucial requirements is to ensure that interference with the right to privacy and data protection through surveillance measures does not exceed the limits of what is strictly necessary. It is of great importance to apply this condition also to AI surveillance measures. Prior to the introduction of surveillance measures, there must be evidence regarding their effectiveness in achieving the particular public interest objective, while the measures chosen should be the least restrictive means for achieving that objective. Many examples show that in practice facial recognition systems are often introduced without considering whether they are "strictly" or "absolutely" necessary and proportionate, furthermore, that they are used secretly without informing individuals and the public. Such practices not only violate the right to privacy, but are also contrary to the rule of law and can have a negative effect on democracy.

The extensive jurisprudence of European supranational courts on mass surveillance clearly shows the importance of human rights organizations and activists in promoting effective safeguards against mass surveillance measures. Many non-governmental organisation and privacy rights activists have initiated strategic cases to protect the interests of society and each individual from being subjected to disproportionate mass surveillance measures. Given that each individual may have limited opportunities to defend their rights, mechanisms for protection of collective interests as perceived by individuals should be strengthened.

752 See EDPB. (2020). Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en.

Chapter 6 analyses data protection requirements and their applications to AI surveillance technologies, in particular facial recognition technology, and the challenges that AI presents to data protection rules. The chapter analyses and compares the requirements set out in EU data protection law – the Law Enforcement Directive that applies to law enforcement authorities and the GDPR, as well as the Council of Europe's Convention108+[753].

Section 1 explains the meaning of personal data and biometric data, pointing out that facial images are considered to be biometric data if they allow unique identification or authentication of a natural person. It discusses the different uses of facial recognition technology, for instance authentication and identification, which is seen as more dangerous, and profiling of individuals based on their personal characteristics. The author argues that suggestions by legal scientists to recognize that new information about a person inferred by algorithmic models can be regarded as personal data have to be supported.[754] It also points out that "real-time" remote facial recognition technology in publicly accessible places poses an even higher risk than "post" systems as the number of false matches increases in uncontrolled public places.

Section 2 examines the principles of personal data processing that lie at the heart of all other data protection requirements. First examined is the principle of lawfulness, which requires a legal basis for processing personal data and allows processing of special categories of data only in certain exceptional and limited circumstances. Public authorities are allowed to process biometric data where this is strictly necessary for reasons of substantial public interests and where they are authorized by law, which must be proportionate, respect the essence of fundamental rights and provide appropriate safeguards. While these are important requirements, countries are left with a wide discretion to decide when the use of facial recognition and other AI surveillance technologies in the public sector is "absolutely necessary and proportionate" to protect substantial public interests.

As for the principle of purpose limitation, there is a risk that personal data – facial images – that are used to train or develop facial recognition technology were originally collected for a different purpose and a legal basis for the new purpose is lacking. It must be ensured that images available in digital format – for example, from social media – could not be processed to obtain biometric

753 Council of Europe. (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data – Consolidated text. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

754 Sartor, G. (2020). The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence. European Parliament. http://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

templates or integrated into biometric systems without a specific legal basis for the new processing when those images were originally taken for other purposes.

Principles of fairness and transparency require that individuals are informed about use of surveillance technology and its purposes, the existence of automated decision-making as well as to provide meaningful information on its logic and expected consequences. At the same time, it is unclear what the logic and consequences of an automated decision mean, as there is a conflict between the need to provide concise and easily understandable information, on the one hand, and accurate and in-depth information, on the other. Likewise, the principle of fairness is linked to concerns about fairness and non-discrimination in automated decision making. Transparency may also require access to data, in particular to the AI system training set, in order to identify possible causes of unfairness or bias resulting from insufficient or biased data or the training algorithm. This is especially important where the algorithmic model is not transparent, as a result of which it is not possible to detect possible mistakes or cases of discrimination. While systematic transparency in law enforcement may hinder crime prevention or the effectiveness of public criminal investigations, at the same time there is a need for some transparency in order to inform individuals about the risks, rules, guarantees and rights regarding processing of their personal data and how to exercise and defend their rights.

The data minimization principle requires that the principle of proportionality be applied in order to evaluate whether it is possible to minimize the amount of data or reduce their "personality" by using appropriate technical means.

The principle of accuracy – requiring that personal data are accurate and, where necessary, kept up to date – also raises challenges with regard to AI surveillance technologies. One of the biggest concerns regarding these technologies is that they are not sufficiently accurate. Moreover, erroneous results are related to data quality and accuracy of data processing. Additionally, members of a particular group may suffer from prejudice if that group is not represented proportionally in the training data, since AI models trained on such data will produce biased predictions towards the underrepresented group.

As for the data security principle, it is emphasized that facial recognition and other biometric technologies pose significant security risks that are difficult or even impossible to predict. Biometric data such as fingerprints and facial images cannot be replaced, unlike other forms of authentication, such as passwords. Thus, biometric data security breaches can have particularly serious consequences for data subjects, as unauthorized disclosure of such sensitive data cannot be corrected. Strict security measures should be implemented at both technical and organizational levels at all stages of processing to protect facial recognition data and image sets against data loss and unauthorized access or use.

In accordance with the principle of accountability, public and private entities must be able to demonstrate compliance of AI systems that rely on processing of personal data with all data protection requirements. They are required to implement appropriate technical and organizational measures, for instance transparency policies and reports, prior impact and accuracy assessment, and integrate data protection into the design and architecture of AI systems.

Section 3 analyses automated decision making and the human oversight requirement. Facial recognition technology algorithms never provide a final result, but only probabilities. Although the accuracy of this technology is increasing, there is always a certain level of error. Decisions that are based solely on this technology – like any other automated processing which produces an adverse legal effect concerning the data subject or significantly affects them – should be prohibited.

Data protection rules in exceptional cases accept such decisions, including those based on biometric data, if they are authorized by law that provides suitable measures to safeguard the rights and freedoms of the data subject, including the right to obtain human intervention on the part of the controller. However, their use should be strictly limited and there should be supervision and impact assessment, for example evaluating whether such decisions do not discriminate against persons on the basis of underrepresented categories before they can be implemented.

The safeguards to be applied in the case of automated decision-making, in particular when biometric data are processed, include the right to obtain human intervention, for the data subject to express their point of view and to contest the decision, the right to be informed of the existence of automated decision-making, including profiling, to obtain meaningful information about the logic involved as well as the significance and expected consequences of such processing for the data subject.

Human oversight – the new requirement introduced in the proposal for an AI Act – is closely linked to the data protection requirement for the right to obtain human intervention in a case of automated decision-making. Human oversight is a vital requirement for use of facial recognition and other AI surveillance technologies and must be ensured in all cases. However, this requirement is not clear. It could be incorrectly implemented as simple validation of all system results, making it fully automated. Opposite cases, when people review and potentially override the system's results, could also raise concerns, since in practice people might tend to override the results of algorithms if the results are in line with their stereotypes, thereby putting minority groups at a disadvantage.[755]

755 Sartor (2020), The Impact of the General Data Protection Regulation ..

Section 4 examines data subject rights and emphasizes that, since facial recognition and other AI surveillance systems are based on processing of personal data, data subjects must be guaranteed all data subject rights: the right to information, which lies at the heart of the principle of transparency, the right not to be the subject of automated decisions, the right of access, the right to object, rectification and erasure of data as well as the right to effective protection of rights.

People often do not know that their facial images are recorded and processed in a database for comparison. If they are not informed and aware of processing, they cannot exercise other rights.

In addition to the right to information, the right to access is also important with regard to AI surveillance measures. Both rights are linked and allow exercise of the right to an effective remedy. Although the data subject's right of access is not the same as the right of access to files or documents, both rights derive from the requirement of good administration and the obligation of any public authority to state reasons for its decisions.

One of the challenges is how to ensure the accuracy of facial recognition systems. In the event of a false match of facial images, data subjects may request corrections to avoid the system re-establishing a false match in the future.

Another difficult question is whether the obligation to delete personal data also includes inferred personal data or inferred group data, such as a trained algorithmic model.

Although the rights of data subjects, including the right to information, the right to access data and the right to delete data can be restricted, for instance arising from obligations of law enforcement authorities to work with a certain degree of confidentiality and secrecy, in order to ensure the effectiveness of their work. However, these restrictions must be laid down by law and must be necessary and proportionate in a democratic society as well as compensated by other safeguards, such as oversight by independent authorities, public supervision, and so on. In this regard, the right to an effective remedy is of particular importance to prevent arbitrary and unlawful data processing. In the event of a restriction, law enforcement authorities must inform individuals, *inter alia*, of the measures taken if the notification is no longer likely to jeopardize their investigations, their right to complain to the supervisory authorities and their right to an effective judicial remedy. This obligation also applies to data used for facial recognition and other surveillance technologies. People may want to dispute that their facial image is on a 'watch list' in case this was done in a non-transparent way and without their consent, or seek redress for a false positive match that has had negative consequences for them such as unlawful detention or arrest as well as claim compensation for any damage caused.

Section 5 examines data protection impact assessment as one of the most important AI accountability tools. The data protection rules require a data protection impact assessment before implementing facial recognition and other biometric surveillance technologies and also require prior consultation with data protection authorities. These requirements play a significant role in preventing implementation of controversial new surveillance technologies that pose high risks to fundamental rights.

Section 6 explores data protection standards for Covid-19 contact tracking apps that have been developed by many international and European organizations. Many of the requirements that were identified during discussions – such as effectiveness, transparency, impact assessment, voluntariness, independent monitoring – are also of particular importance with regard to AI surveillance technologies. The speed with which a wide range of stakeholders – scientists, technology companies, civil society organizations, international organizations – were involved and collaborated to develop standards for the implementation and evaluation of these apps could serve as a good example of how to evaluate legal compliance of other new technologies.

Chapter 7 is the final chapter, summarizing the discussion and the main findings and providing recommendations for further development of AI regulation based on human rights. It also advises what governance mechanisms and safeguards need to be put in place to ensure responsible and trustworthy use of AI systems and to prevent risks and threats to human rights, democracy and the rule of law.

Section 1 "beyond ethical principles" emphasizes that discussions on regulation of AI have so far mainly focused on ethical principles and mostly offer general recommendations and suggestions, rather than how to develop effective enforcement mechanisms and a framework for their practical implementation. Therefore, regulation needs to go further. Agreeing on common and internationally recognized moral norms is essential, as they provide ideals, inspire action, and mark a clearer direction for AI development that will serve and bring benefits to humanity and society. However, AI regulation cannot be based solely on AI ethical principles. Methods and tools must be identified to put ethical values and principles into practice. In this regard, legal requirements play a crucial role. It is necessary to define a set of harmonized rules that constitute the minimum requirements to be met in order for AI systems to be recognized as ethical and legitimate. Human rights lie at the heart of ethical principles, and respect for them in the context of democracy and the rule of law is the most secure way of defining abstract ethical principles and values.

Section 2 further explains that human rights form the cornerstone of AI regulation. International human rights law establishes global standards, that

is, a universal set of rules and minimum standards, based, *inter alia*, on human dignity, autonomy, equality and the rule of law, that determine how people should be treated. These standards and related legal mechanisms create clear legal obligations for states to respect, protect and implement human rights. They also require that persons whose rights have been denied or violated have the right to an effective legal remedy.

Human rights form the basis of AI regulation and play a key role in the further development of the international and EU AI legal framework. This has been emphasized in many AI ethical guidelines developed by international organizations, such as the Council of Europe[756], the EU[757] and UNESCO[758] as well as by academic researchers[759]. There are many advantages to using human rights-based regulation in the context of AI. Over time, a broad human rights protection system has been established at the international, regional and national levels where individuals can seek legal remedies in the case of human rights violations. There is established case-law on how to interpret and apply these remedies in specific situations. Human rights provide a universal language for global issues and they are internationally recognized.

At the same time, there are also challenges to implementing a human rights-based approach to AI. Human rights are more oriented towards states than private actors. They are better suited for reducing significant harm to a small number of people than for preventing harm to the collective interest. AI, including surveillance systems and their effects on human rights and freedoms, is more difficult to challenge individually. At the societal level, joint and coordinated action is needed to protect privacy and autonomy as a public good.[760]

Within the European human rights protection system, a human rights-based AI regulatory framework could be established as a model for the rest of the world. The EU is founded on the values of human dignity, freedom, democracy, the rule of law and respect for human rights. The EU could create a "gold standard" in the form of regulation for a human rights-based AI that would be directly applicable in all Member States, similar to EU data protection rules. The Council of Europe as the continent's leading human rights institution could also develop

756 Council of Europe, CAHAI Secretariat (2020), Towards regulation of AI systems.

757 European Commission (2020), White Paper. On Artificial Intelligence.

758 UNESCO (2022), Recommendation on the Ethics of Artificial Intelligence.

759 Mantelero, A. (2020). Regulating AI within the Human Rights Framework: A Roadmapping Methodology. In: Czech, P., Hesch, L., Lukas, K., Nowak, M., Oberleitner, G. (eds.), *European Yearbook on Human Rights. Interesentia*, pp. 477–502.

760 See Taylor, L., van der Sloot, B., Floridi, L. (2017). Conclusion: What Do We Know About Group Privacy? In: *Group Privacy*, Taylor, L., Floridi, L., van der Sloot, B. (eds.), Cham: Springer International Publishing, pp. 225–37.

a clear framework based on human rights, the rule of law and democratic values by adopting a new legally binding instrument, such as a framework convention. Future legal regulation of AI should further develop human rights norms by clarifying their application to specific use cases. It should be built on existing human rights instruments, but also go beyond them, in order to adapt and contextualize the application of these rights and freedoms and address the shortcomings of legislation created before the AI era.[761]

Section 3 emphasizes the need for new AI regulation. The need for a clear legal framework for AI has been increasingly acknowledged by international organisations, including the EU and the European Council. Although existing legal norms, in particular human rights and data protection law, already regulate AI, this regulation has a number of shortcomings. Firstly, the rights and obligations set out in existing legal instruments are usually formulated broadly or in general terms, and it may be difficult to interpret them in relation to AI systems. Moreover, they clearly do not address some issues related to AI. Secondly, a number of key requirements and safeguards related to protection of human rights, democracy and the rule of law in the AI field are currently not explicitly enshrined in law – for instance human control, supervision, transparency and accountability. Thirdly, current instruments also do not pay enough attention to the steps that developers and deployers of AI systems need to take to ensure the effectiveness of AI systems whenever they may have an impact on human rights, democracy or the rule of law as well as to ensure that they have the necessary competences or professional qualification.

Existing human rights and data protection norms should be adapted to the specificities of the field. A new legal framework for AI could combine adoption of a new general legally binding instrument with sectoral instruments, both legally binding and non-binding, that would address specific sectoral challenges of AI, especially in high-risk areas such as law enforcement.[762] While human rights and data protection legislation lay down important requirements for the development and use of AI surveillance technologies, in particular facial recognition technology, new specific rules need to developed and adopted that would clarify how these existing rules should be applied to surveillance activities for law enforcement purposes.

761 Mantelero (2020), Regulating AI within the Human Rights Framework, pp. 477–502.

762 Council of Europe. (2020). Ad Hoc Committee on Artificial Intelligence (CAHAI) Feasibility Study. https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da.

Section 4 argues that red lines should be drawn on mass surveillance and clearly set in forthcoming AI regulation.[763] AI systems should not be used for mass surveillance. The AI legal framework should include a prohibition on indiscriminate use of facial recognition and other biometric surveillance technologies that could lead to mass surveillance in public or publicly accessible spaces. Law enforcement authorities do not need to carry out mass surveillance in order to ensure citizens' security or safety, as surveillance should always be targeted as well as strictly necessary and proportionate. Facial recognition technology is often used unlawfully and discriminatorily in both public and private sectors. These practices may cause significant harm and violate fundamental rights and democratic principles. A moratorium on targeted use of facial recognition technologies should be introduced. In like manner, this concerns other types of AI technologies posing high risks to fundamental rights, the rule of law and democracy. Their effectiveness and benefit to society should be clearly demonstrated to prevent arbitrary and unlawful use. Emotional recognition systems drawing conclusions and predictions about our behaviours, thoughts and other personal characteristics as well as biometric categorisation systems should likewise be prohibited by law, since the use of such technologies in itself violates human dignity, autonomy and other fundamental rights. Similarly, use of AI-enabled predictive policing methods by law enforcement authorities such as AI systems intended to be used for predicting the occurrence or reoccurrence of criminal offences based on profiling of a natural person or on assessing personality traits and characteristics or past criminal behaviour should not be allowed. AI-enabled social scoring and manipulation or control of human behaviour should be prohibited by law as well, since these practices pose significant threats to fundamental democratic principles and freedoms.

It is important not to miss the crucial moment when international and European organisations, as well as national legislators, are developing AI legal regulation and when it is possible to prohibit uses of AI systems that pose significant risks and threats to human rights, the rule of law and democracy. International organisations are increasingly recognising the importance of introducing clear limitations on certain uses of AI technologies that violate and pose threats to human rights, the rule of law and democracy, at the same time hesitating to propose specific legal provisions. It is of paramount importance to legally

763 See ibid.; EDRi. (17 February, 2021). New ECI calls Europeans to stand together for a future free from harmful biometric mass surveillance. https://edri.org/our-work/new-eci-ban-biometric-mass-surveillance/; Council of Europe. Ad Hoc Committee on Artificial Intelligence (CAHAI). (2020). The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law. Report by Muller C. https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da.

impose clear legal restrictions in the forthcoming AI legal framework at both the international and EU regulation levels. The EU, the Council of Europe as well as other international organisations should gain momentum while there remains a real opportunity to introduce strict restrictions in forthcoming AI regulation. It is not even a question of whether we might want or accept a particular use of AI systems or not. Clear restrictions, prohibitions or a moratorium would not constitute new red lines, but rather ensure recognition of existing ones. It must be acknowledged that use of AI surveillance technologies for mass surveillance already violates our dignity, fundamental rights and freedoms and democratic principles. If the new AI legal framework lacks such prohibitions and restrictions, it will be very hard to prevent mass surveillance measures from becoming the new normal in the decades to come. While discussions are still open, we are obliged to take persuasive steps in order to protect human rights, the rule of law and democracy.

Section 5 argues that impact assessment is one of the main AI accountability mechanisms that has been widely supported by international and European organisations[764], governments[765], academics[766] and other organisations. AI impact assessment can be an important accountability tool to ensure that institutions and companies are aware of – and assess – the risks of AI technologies and evaluate their wider impact on human rights, the rule of law, democracy, as well as social, ethical and other implications. It can also be an effective tool for informing the public and individuals about the use of such AI systems.

However, a risk-based approach to AI regulation is not enough to protect human rights. AI should not be regulated on the basis of risk, but on the basis of human rights. Regulation should not require only institutions and companies themselves to assess the risks of AI surveillance technologies to human rights, society and democracy but rather this should be done by an independent third party, because both public authorities and companies may have an interest in underplaying risks in the development, implementation and use of AI technologies. Although the EU data protection framework already imposes an obligation to assess the impact of AI technologies on individual rights and freedoms, many cases show that this requirement does not effectively prevent introduction of AI surveillance technologies violating data protection rules and human rights law.[767]

764 Council of Europe Commissioner for Human Rights (2019), Unboxing Artificial Intelligence ..

765 Government of Canada, Algorithmic Impact Assessment.

766 Mantelero (2018), AI and Big Data ..; Reisman et al. (2018), Algorithmic Impact Assessments Report.

767 EDPB (21 February, 2021), Swedish DPA ..; EDPB. (22 August, 2019). Facial recognition in school renders Sweden's ..

Human rights are non-negotiable and must be respected regardless of the level of risk.

Section 6 examines independent oversight and public participation as important safeguards to ensure AI accountability. Control by an independent supervisory authority, as well as public oversight, is particularly important for high-risk AI technologies, such as facial recognition and other biometric surveillance technologies. In order to ensure accountable use of AI technologies and to prevent the threats they raise, it is necessary to establish an effective, transparent, inclusive monitoring and independent oversight mechanism.[768] At European level, many proposals have been made to set up an independent supervisory authority to monitor the use of AI systems and its compliance with human rights and other legal requirements. It is also important to recognize the crucial role of existing national authorities, in particular data protection authorities, human rights authorities and ombudsman institutions to ensure effective monitoring of AI systems. National supervisory authorities must be provided with sufficient resources, powers and competences to prevent and assess violations of fundamental rights, and to provide effective support to those whose human rights are affected by AI systems.

Effective monitoring of AI systems requires close cooperation amongst a broad range of relevant stakeholders, including public authorities, private actors, academics and civil society organizations representing the interests of different groups. Public participation with the active engagement of individuals and groups potentially affected should also be included in the impact assessment of controversial AI technologies by involving the individuals and groups these technologies may prospectively affect.[769] When conducting AI impact assessment, supervisory authorities should organise consultations with different stakeholders and experts in various fields, such as computer sciences, data sciences, health and behavioural sciences, social sciences, ethics and law. It is not the police or other law enforcement authorities that are planning to use AI surveillance technologies, but independent supervisory authorities, with the assistance of individuals, groups and other stakeholders, that should evaluate whether the systems should be used and *ex ante* assess the balance between privacy and security interests. Monitoring and independent oversight together with public participation mechanisms are essential to prevent the development, deployment and use of AI surveillance technologies that violate human rights, other legal requirements

768 Council of Europe, CAHAI (2020), Feasibility Study.

769 Ibid.; European Parliament (2020), Report with recommendations to the Commission on a framework ..; Mantelero (2020), Regulating AI within the Human Rights Framework, pp. 477–502.

and democratic values. These mechanisms are essential for meeting people's expectations on acceptable use of AI technologies as well as for identifying and introducing red lines for undesirable and harmful technologies.

Independent monitoring and public participation are the safeguards for a so-called strategic level of supervision. There is also a tactical level of supervision, which sets out the rules that have been adopted for use of the system for certain purposes and defines the requirements to be met in each individual case. An essential requirement for surveillance technology is prior approval or warrant by an independent judge, which can authorize targeted use of surveillance technology for national security purposes. Such a safeguard as an important guarantee against unfair practices and abuses of power also stems from the extensive mass surveillance case-law of the ECtHR and the CJEU.

Section 7 explores transparency and awareness as crucial AI safeguards. Use of AI systems is often hidden or unknown, making it difficult or impossible to assess their impact and monitor their use. If individuals and society are unaware of the use of AI surveillance systems, they cannot know about infringement of their rights and freedoms and ensure their protection. The legal framework should include clear transparency requirements. For example, a legal obligation to publish an impact assessment of AI systems as well as public consultation results reflecting the views of experts and members of the public, particularly regarding high-risk technologies. The requirement for AI developers and deployers to make available information in order to enable the supervisory authority to assess AI systems should also be introduced. The supervisory authority should also educate and raise public awareness of AI implications, risks, threats and accountability requirements.

One proposal that would make a significant contribution to transparency is to establish a register of AI systems.[770] The register could be set up at the national level as well as at the EU level and include information about use of AI systems by public institutions and in high-risk sectors, with uses or purposes including law enforcement, migration, border control, and the judicial sectors in all EU Member States.

Awareness and education are essential to create trust as a precondition for AI systems to be used and accepted. First of all, we need to raise public awareness that will lead to action, that is, call for AI systems that bring benefits to society and do not pose risks and threats to rights and freedoms. Education and awareness-raising are the precondition for individuals to be aware of their values and rights and to be able to protect them.

770 See, e.g., Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence.

Finally, **Section 8** highlights the importance of closely monitoring developments in digital technologies introduced in response to Covid-19. The crisis has made the decision-making process of governments, including adoption of new technologies and other restrictive measures, far less democratic but more secretive and non-transparent – a state of affairs that could be difficult to reverse. Countries should introduce a regulatory framework that would ensure monitoring, independent oversight mechanisms, clear requirements for transparency and impact assessment of development, deployment and use of new technologies in the public interest. These rules imposing an obligation to comply with the above-mentioned requirements would significantly reduce the possibility that countries could introduce new, highly intrusive technologies without prior assessment of their efficiency and their legal, ethical and societal impact. Likewise, such rules would prevent further use of existing technologies for completely different and unforeseen purposes. Clear regulation and control mechanisms are essential not only to protect human rights and democratic values, but also to prevent mass surveillance measures from becoming the new norm in the post-Covid-19 era. However, along with many challenges the crisis has created a unique opportunity to re-evaluate democratic governance policies and processes. It may also encourage critical assessment of the capabilities and efficiency of AI and other new technologies, and help to recognize the impact of these technologies on our rights and freedoms. Crises can also foster the development of trustworthy and human-centric AI that puts human rights, the rule of law and democracy at the forefront.

Izmantotie avoti

TIESĪBU AKTI

Starptautiskie līgumi

ANO līgumi

Apvienoto Nāciju Organizācijas Statūti. Pieņemti 26.06.1945. (Latvijā spēkā no 17.09.1991.). *Latvijas Vēstnesis*, 29.01.2018. Nr. 20.

Bērnu tiesību konvencija. Pieņemta 20.11.1989. (Latvijā spēkā no 14.05.1992.). *Latvijas Vēstnesis*, 28.11.2014., Nr. 237.

Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām. Pieņemts 16.12.1966. (Latvijā spēkā no 14.07.1992). *Latvijas Vēstnesis*, 23.04.2003., Nr. 61.

Vispārējā cilvēktiesību deklarācija. Pieņemta 10.12.1948. (Latvijā spēkā no 22.05.1990.). https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/lat.pd

Eiropas Padome

Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija. Pieņemta 04.11.1950. (EP, Latvijā spēkā no 27.06.1997.). *Latvijas Vēstnesis*, 13.06.1997., Nr. 144/145.

Konvencija par kibernoziegumiem. Pieņemta 23.11.2001. (EP, Latvijā spēkā no 01.06.2007.). *Latvijas Vēstnesis,* 26.10.2001., Nr. 171.

Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi. Pieņemta 28.01.1981. (EP, Latvijā spēkā no 01.09.2001.). *Latvijas Vēstnesis*, 12.04.2001., Nr. 59.

Protokols, ar ko groza Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu apstrādi. *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Pieņemts 10.10.2018. https://rm.coe.int/16808ac918

Eiropas Savienības tiesību akti

Eiropas Savienības Pamattiesību harta. Pieņemta 07.12.2000. OV C 2020/239, 07.06.2016.

Līgums par Eiropas Savienības darbību (konsolidētā versija). OV C 326/47. 26.10.2012.

Līgums par Eiropas Savienību, 1992. OV C 325, 24.12.2002.

Līgums par Eiropas Savienību (konsolidētā versija), OV C 115/13, 09.05.2008.

Nolīgums starp Amerikas Savienotajām Valstīm un Eiropas Savienību par pasažieru datu reģistra datu izmantošanu un pārsūtīšanu Amerikas Savienoto Valstu Iekšzemes drošības departamentam. OV L 215, 11.08.2012.

Nolīgums starp Eiropas Savienību un Amerikas Savienotajām Valstīm par tādu finanšu ziņojumapmaiņas datu apstrādi un nodošanu, kurus Eiropas Savienība dara pieejamus Amerikas Savienotajām Valstīm, lai īstenotu Teroristu finansēšanas izsekošanas programmu. OV L 8, 13.01.2010. (spēkā līdz 31.10.2010.).

Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti. *OV L* 281, 23.11.1995.

Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju). *OV L* 201, 31.07.2002.

Eiropas Parlamenta un Padomes Direktīva 2006/24/EK (2006. gada 15. marts) par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK. *OV L* 105, 13.04.2006. (spēkā līdz 03.05.2006).

Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI. *OV L* 119, 04.05.2016.

Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā. *OV L* 194, 19.07.2016.

Eiropas Parlamenta un Padomes Direktīva (ES) 2019/1024 (2019. gada 20. jūnijs) par atvērtajiem datiem un publiskā sektora informācijas atkalizmantošanu. *OV L* 172, 26.06.2019.

Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (Dokuments attiecas uz EEZ). *OV L* 119, 04.05.2016.

Eiropas Parlamenta un Padomes Regula (ES) 2016/794 (2016. gada 11. maijs) par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu) un ar kuru aizstāj un atceļ Padomes Lēmumus 2009/371/TI, 2009/934/TI, 2009/935/TI, 2009/936/TI un 2009/968/TI. *OV L* 135, 24.05.2016.

Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK. *OV L* 295/39, 21.11.2018.

Eiropas Parlamenta un Padomes Regula (ES) 2018/1727 (2018. gada 14. novembris) par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (*Eurojust*) un ar ko aizstāj un atceļ Padomes Lēmumu 2002/187/TI. *OV L* 295, 21.11.2018.

Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā. *OV L* 303/59, 28.11.2018.

Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (Dokuments attiecas uz EEZ). *OV L* 151, 07.06.2019.

Eiropas Parlamenta un Padomes Regula (ES) 2022/868 (2022. gada 30. maijs) par Eiropas datu pārvaldību un ar ko groza Regulu (ES) 2018/1724 (Datu pārvaldības akts) (Dokuments attiecas uz EEZ). *OV L* 152, 03.06.2022.

Eiropas Parlamenta un Padomes Regula (ES) 2022/1925 (2022. gada 14. septembris) par sāncensīgiem un godīgiem tirgiem digitālajā nozarē un ar ko groza Direktīvas (ES) 2019/1937 un (ES) 2020/1828 (Digitālo tirgu akts) (Dokuments attiecas uz EEZ). *OV L* 265, 12.10.2022.

Eiropas Parlamenta un Padomes Regula (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts) (Dokuments attiecas uz EEZ). *OV L* 227, 27.10.2022.

Komisijas Ieteikums (ES) 2020/518 (2020. gada 8. aprīlis) par vienotu Savienības rīkkopu tehnoloģiju un datu izmantošanai ar mērķi apkarot Covid-19 krīzi un iziet no tās, it īpaši attiecībā uz mobilajām lietotnēm un anonimizētu mobilitātes datu izmantošanu. *OV L* 114/7, 14.04.2020.

Padomes Regula (ES) 2017/1939 (2017. gada 12. oktobris), ar ko īsteno ciešāku sadarbību Eiropas Prokuratūras (EPPO) izveidei. *OV L* 283, 31.10.2017.

Latvijas tiesību akti

Latvijas Republikas Satversme. Pieņemta 15.02.1922. (spēkā no 07.11.1922.). Latvijas Vēstnesis, 01.07.1993., Nr. 43.

Elektronisko sakaru likums. Pieņemts 28.10.2004. *Latvijas Vēstnesis*, 17.11.2004., Nr. 183.

Fizisko personu datu apstrādes likums. Pieņemts 21.06.2018. *Latvijas Vēstnesis*, 04.07.2018., Nr. 132.

Informācijas sabiedrības pakalpojumu likums. Pieņemts 04.11.2004. *Latvijas Vēstnesis*, 17.11.2004., Nr. 183.

Informācijas tehnoloģiju drošības likums. Pieņemts 28.10.2010. *Latvijas Vēstnesis*, 10.11.2010., Nr. 178.

Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā. LV likums. Pieņemts 08.07.2019. *Latvijas Vēstnesis*, 22.07.2019., Nr. 147.

MK noteikumi Nr. 442. Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām. Pieņemti 28.07.2015. Latvijas Vēstnesis, 03.08.2015., Nr. 149.

Eiropas Savienības tiesību aktu projekti

Eiropas Komisija. (2017). Priekšlikums. Eiropas Parlamenta un Padomes regula par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula). https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX:52017PC0010

Eiropas Komisija. (2020). Priekšlikums. Eiropas Parlamenta un Padomes regula par saskaņotiem noteikumiem par taisnīgu piekļuvi datiem un to lietošanu (Datu akts). https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52022PC0068

Eiropas Komisija. (2021). Priekšlikums. Eiropas Parlamenta un Padomes regula, kas nosaka saskaņotas normas mākslīgā intelekta jomā (Mākslīgā intelekta akts) un groza dažus Savienības leģislatīvos aktus. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

Eiropas Komisija. (2021). Priekšlikums. Eiropas Parlamenta un Padomes regula par sadarbspējīgu vakcinācijas, testēšanas un pārslimošanas sertifikātu izdošanas, verifikācijas un akceptēšanas satvaru nolūkā atvieglot brīvu pārvietošanos Covid-19 pandēmijas laikā (digitālais zaļais sertifikāts). https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52021PC0130&from=EN

JURIDIKATŪRA

Eiropas Cilvēktiesību tiesas spriedumi

ECT 1978. gada 6. septembra spriedums lietā 5029/71 *Klass and Others v. Germany.*
ECT 1984. gada 2. augusta spriedums lietā 8691/79 *Malone v. The United Kingdom.*
ECT 1990. gada 24. aprīļa spriedums lietā 11105/84 *Huvig v. France.*
ECT 2000. gada 16. februāra spriedums lietā 27798/95 *Amann v. Switzerland*.
ECT 2006. gada 29. jūnija lēmums lietā 54934/00 *Weber and Saravia v. Germany.*
ECT 2007. gada 28. jūnija spriedums lietā *The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria.*
ECT 2007. gada 3. aprīļa spriedums lietā 62617/00 *Copland v. The United Kingdom.*
ECT 2008. gada 4. decembra spriedums lietās 30562/04 un 30566/04 *Marper v. the United Kingdom.*
ECT 2010. gada 18. maija spriedums lietā 26839/05 *Kennedy v. The United Kingdom.*
ECT 2010. gada 2. septembra spriedums lietā *Uzun v. Germany*.
ECT 2015. gada 4. decembra spriedums lietā 47143/06 *Roman Zakharov v. Russia.*
ECT 2016. gada 12. janvāra spriedums lietā 37138/14 *Szabó and Vissy v. Hungary.*
ECT 2017. gada 18. jūlija spriedums lietā 27473/06 *Mustafa Sezgin Tanrıkulu v. Turkey.*
ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13, 62322/14, 24960/15 *Big Brother Watch and Others v. The United Kingdom.*
ECT 2018. gada 19. jūnija spriedums lietā 35252/08 *Centrum för Rättvisa v. Sweden.*
ECT 2020. gada 13. februāra spriedums lietā 45245/15 *Gaughran v. The United Kingdom.*

Eiropas Savienības Tiesas nolēmumi

EST 1978. gada 31. janvāra spriedums lieta 94/77 *Fratelli Zerbone Snc* pret *Amministrazione delle finanze dello Stato*, ECLI:EU:C:1978:17.
EST 2009. gada 7. maija spriedums lietā C553/07 *Rijkeboer*, ECLI:EU:C:2009:293.
EST 2013. gada 17. oktobra spriedums lietā C-291/12, *M. Schwarz* pret *Stadt Bochum*, ECLI:EU:C:2013:670.
EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C293/12 *Digital Rights Ireland* un C594/12 *Seitlinger* u. c., ECLI:EU:C:2014:238.
EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems* pret *Data Protection Commissioner*, ECLI:EU:C:2015:650.
EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15 *Tele2 Sverige AB* un C-698/15 *Watson* u. c., ECLI:EU:C:2016:970.
EST 2017. gada 26. jūlija atzinums 1/15 *Accord PNR UE-Canada*, ECLI:EU:C:2017:592.
EST 2020. gada 16. jūlija spriedums lietā C-311/18 *Data Protection Commissioner* pret *Facebook Ireland Limited* un *Maximillian Schrems*, ECLI:EU:C:2020:559.
EST 2020. gada 6. oktobra spriedums apvienotajās lietās C511/18 *La Quadrature du Net* u. c., C-512/18 *French Data Network* u. c. un C-520/18 *Ordre des barreaux francophones et germanophone* u. c., ECLI:EU:C:2020:791.
EST 2020. gada 6. oktobra spriedums lietā C-623/17 *Privacy International*, ECLI:EU:C:2020:790.

Latvijas Republikas Satversmes tiesas spriedumi un lēmumi

Satversmes tiesas 2012. gada 20. aprīļa sprieduma lietā Nr. 2011-16-01.
Satversmes tiesas 2016. gada 16. marta spriedumu lietā Nr. 2015-14-0103.
Satversmes tiesas 2019. gada 5. marta spriedums lietā Nr. 2018-08-03.

Satversmes tiesas 2019. gada 6. marta spriedums lietā Nr. 2018-11-01.
Satversmes tiesas 2020. gada 18. novembra spriedums lietā Nr. 2019-32-01.
Satversmes tiesas 2020. gada 20. novembra spriedums lietā Nr. 2019-33-01.
Satversmes tiesas 2022. gada 18. februāra lēmums lietā Nr. 2021-10-03.

STARPTAUTISKO ORGANIZĀCIJU DOKUMENTI

Apvienoto Nāciju Organizācija (ANO)

ANO Ģenerālās Asamblejas rezolūcija

UN General Assembly. (2013). Resolution 68/167. The right to privacy in the digital age. https://digitallibrary.un.org/record/764407/?ln=en

ANO ģenerālsekretāra stratēģija

UN. (2018). UN Secretary-General's Strategy on new technologies. https://www.un.org/en/newtechnologies/images/pdf/SGs-Strategy-on-New-Technologies.pdf

ANO Augstā cilvēktiesību komisāra birojs

OHCHR. (2014). The right to privacy in the digital age. https://digitallibrary.un.org/record/777869
OHCHR. (2011). Guiding Principles on Business and Human Rights. Implementing the United Nations "Protect, Respect and Remedy" Framework. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
OHCHR. (2018). The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. https://digitallibrary.un.org/record/777869#record-files-collapse-header

ANO Rasu diskriminācijas izskaušanas komiteja

UN Committee on the Elimination of Racial Discrimination. (2020). General recommendation No. 36. Preventing and Combating Racial Profiling by Law Enforcement Officials. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/349/50/PDF/G2034950.pdf?OpenElement

ANO Cilvēktiesību padome un ANO īpašais referents jautājumos par uzskatu un vārda brīvības tiesību veicināšanu un aizsardzību

UN Human Rights Council. (2019). Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. https://digitallibrary.un.org/record/3814512#record-files-collapse-header

ANO īpašais referents par tiesībām uz privātumu

UN Special Rapporteur on the right to privacy. (2017). Report of the Special Rapporteur on the right to privacy. https://digitallibrary.un.org/record/3845912
UN Special Rapporteur on the right to privacy. (2018). Report of the Special Rapporteur on the right to privacy. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/324/47/PDF/G1832447.pdf?OpenElement
UN Special Rapporteur on the right to privacy. (2019). Right to privacy. Report of the Special Rapporteur on the right to privacy. https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08;%20https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx

UN Special Rapporteur on the right to privacy. (2020). Draft for Consultations. Data Privacy Guidelines for the development and operation of Artificial Intelligence solutions. https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2020_Sept_draft_data_Privacy_guidelines.pdf

UN Special Rapporteur on the right to privacy. (2020). Report of the Special Rapporteur on the right to privacy. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/071/66/PDF/G2007166.pdf?OpenElement

Apvienoto Nāciju Izglītības, zinātnes un kultūras organizācija (UNESCO)

UNESCO, AHEG. (2020). Outcome document: first draft of the Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000373434

UNESCO. (2020). Composition of the Ad Hoc Expert Group (AHEG) for the Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000372991

UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137

Apvienoto Nāciju Starptautiskais Bērnu fonds (UNICEF)

UNICEF. (2020). Policy guidance on AI for children. https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

ANO Narkotiku un noziedzības novēršanas birojs (UNODC)

UNODC. (2009). Current practices in electronic surveillance in the investigation of serious and organized crime. https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf

ANO Starpreģionālais noziedzības un tieslietu pētniecības institūts (UNICRI) un Starptautiskā Kriminālpolicijas organizācija (INTERPOL)

UNICRI & INTERPOL. (2019). Artificial Intelligence and Robotics for Law Enforcement. https://unicri.it/artificial-intelligence-and-robotics-law-enforcement

Starptautiskā telekomunikāciju savienība (ITU)

ITU. (2015). Recommendation Y.3600. Big data – Cloud computing based requirements and capabilities. https://www.itu.int/rec/T-REC-Y.3600-201511-I/en

Ekonomiskās sadarbības un attīstības organizācija (OECD)

OECD. (1980). Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

OECD. (2013). The OECD Privacy Framework. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

OECD. (2017). OECD Digital Economy Outlook 2017. https://doi.org/10.1787/9789264276284-en

OECD. (2019). Artificial Intelligence in Society. https://www.oecd.org/publications/artificial-intelligence-in-society-eedfee77-en.htm

OECD. (2019). Recommendation of the Council on Artificial Intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

OECD. (2020). Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics. https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics/

Eiropas Padome

Council of Europe. (1981). Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/16800ca434

Council of Europe. (2017). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (T-PD). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. https://rm.coe.int/16806ebe7a

Council of Europe. (2018). Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/16808ac91a

Council of Europe. (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data – Consolidated text. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

Council of Europe. (2019). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). Guidelines of Artificial Intelligence and Data Protection. https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

Council of Europe (2019). Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes. https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4b

Council of Europe. (2019). Report on Artificial Intelligence and Data Protection: Challenges and Possible Remedies. https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6

Council of Europe. (2020). Digital Solutions to fight COVID-19. 2020 Data Protection Report. https://rm.coe.int/report-dp-2020-en/16809fe49c

Council of Europe. (2020). Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services. Joint statement by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb

Council of Europe. (2020). Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. https://rm.coe.int/covid19-joint-statement/16809e09f4

Council of Europe. (2020). Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

Council of Europe. (2020). Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis. https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40

Council of Europe. (2021). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). Guidelines on Facial Recognition. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

Council of Europe, CAHAI. (2020). Feasibility Study. https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

Council of Europe, CAHAI. (2020). The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law. Report by Muller C. https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da

Council of Europe, CAHAI Secretariat. (2020). Towards regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law. https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a

Council of Europe Commissioner for Human Rights. (2019). Unboxing Artificial Intelligence: 10 steps to protect Human Rights. Recommendation. https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

Council of Europe. Committee of Experts on Internet Intermediaries (MSI-NET). (2018). Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

Council of Europe. Committee of Ministers. (1973). Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830

Council of Europe. Committee of Ministers. (1974). Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51

Parliamentary Assembly of the Council of Europe. (1968). Recommendation 509. Human rights and modern scientific and technological developments. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en

Parliamentary Assembly of the Council of Europe. (2015). Resolution 2045. Mass surveillance. http://assembly.coe.int/nw/xml/xref/xref-xml2html-en.asp?fileid=21692&lang=en

Parliamentary Assembly of the Council of Europe. (2017). Recommendation 2102. Technological convergence, artificial intelligence and human rights. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en

Eiropas Cilvēktiesību tiesa (ECT)

European Court of Human Rights. (2020). Guide on Article 8 of the Convention – Right to respect for private and family life. https://www.echr.coe.int/documents/guide_art_8_eng.pdf

Eiropas Savienība (ES)

Eiropas Parlaments

Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_LV.html#title2

Eiropas Parlamenta 2021. gada 25. marta normatīvā rezolūcija par priekšlikumu Eiropas Parlamenta un Padomes regulai, ar ko izveido Savienības režīmu divējāda lietojuma preču eksporta, pārvadājumu, starpniecības, tehniskās palīdzības un tranzīta kontrolei (pārstrādāta redakcija). https://www.europarl.europa.eu/doceo/document/TA-9-2021-0101_LV.html

European Parliament. (2020). Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies. https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html

European Parliament. Committee on Civil Liberties, Justice and Home Affairs (LIBE). (2020). Draft Report on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)), LIBE, Rapporteur Tudor Ciuhodaru. https://www.europarl.europa.eu/doceo/document/LIBE-PR-652625_EN.pdf

Eiropas Komisija

European Commission. (2019). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Building Trust in Human Centric Artificial Intelligence. https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence

European Commission. (2020). Inception Impact Assessment. Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Requirements-for-Artificial-Intelligence

European Commission. (2020). Joint Communication to the European Parliament, the European Council and the Council. A new EU-US agenda for global change. https://ec.europa.eu/info/sites/default/files/joint-communication-eu-us-agenda_en.pdf

European Commission. (2020). White Paper. On Artificial Intelligence – A European approach to excellence and trust. https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European Commission. Expert Group on Liability and New Technologies – New Technologies Formation. (2019). Liability for Artificial Intelligence and Other Emerging Digital Technologies. https://op.europa.eu/publication/manifestation_identifier/PUB_DS0319853ENN

Eiropas Komisija. (2015). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Digitālā vienotā tirgus stratēģija Eiropai. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex%3A52015DC0192

Eiropas Komisija. (2018). Komisijas paziņojums Eiropas Parlamentam, Eiropadomei, Padomei, Eiropas Ekonomikas un sociālajai komitejai un Reģionu komitejai. Koordinētais mākslīgā intelekta plāns. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52018DC0795&from=EN

Eiropas Komisija. (2018). Komisijas paziņojums. Mākslīgais intelekts Eiropai. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52018DC0237&from=EN

Eiropas Komisija. (2020). Baltā grāmata par mākslīgo intelektu. Eiropiska pieeja – izcilība un uzticēšanās. https://op.europa.eu/lv/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

Eiropas Komisija. (2020). Komisijas paziņojums. Norādījumi par lietotnēm, kas sniedz atbalstu cīņā pret Covid-19 pandēmiju saistībā ar datu aizsardzību. *OV C* 124/1, 17.04.2020. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020XC0417(08)&from=EN

Eiropas Komisija (2020). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Eiropas Datu stratēģija. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52020DC0066

Eiropas Komisija (2020). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Eiropas digitālās nākotnes veidošana. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52020DC0067

Eiropas Komisija. (2020). Komisijas ziņojums Parlamentam, Padomei un Eiropas Ekonomikas un sociālo lietu komitejai. Ziņojums par mākslīgo intelektu, lietu internetu un robotiku drošuma un atbildības aspektā. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020DC0064&from=en

Eiropas Komisija. (2020). Kopīgais Eiropas ceļvedis Covid-19 ierobežošanas pasākumu atcelšanai 2020/C 126/01. https://op.europa.eu/lv/publication-detail/-/publication/14188cd6-809f-11ea-bf12-01aa75ed71a1

Eiropas Savienības Mākslīgā intelekta augsta līmeņa ekspertu grupa (AI HLEG)

AI HLEG. (2019). A definition of artificial intelligence: main capabilities and scientific disciplines. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

AI HLEG. (2019). Ethics Guidelines for Trustworthy AI. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

AI HLEG. (2019). Policy and investment recommendations for trustworthy Artificial Intelligence. https://www.europarl.europa.eu/italy/resource/static/files/import/intelligenza_artificiale_30_aprile/ai-hleg_policy-and-investment-recommendations.pdf

AI HLEG. (2020). Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment. https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

Eiropas Datu aizsardzības kolēģija (Europen Data Protection Board, EDPB), Eiropas Datu aizsardzības uzraudzītājs (European Data Protection Supervisor, EDPS)

EDPS. (2015). Opinion 4/2015 Towards a New Digital Ethics Data, Dignity and Technology. https://edps.europa.eu/sites/default/files/publication/15-09-11_data_ethics_en.pdf

EDPS. (2018). Opinion 3/2018. EDPS Opinion on online manipulation and personal data. https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

EDPS. (2019). EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en

EDPB. (2019). Guidelines 3/2019 on processing of personal data through video devices. Version for public consultation. Adopted on 10 July 2019. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

EDPB. (2019). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

EDPB. (10 June, 2020). Response to MEPs Sophie in ‘t Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI. https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en

EDPB. (2020). Guidelines 3/2019 on processing of personal data through video devices. Version 2.0. Adopted on 29 January 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

EDPB, EDPS. (2021). EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate). https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042021-proposal_en

EDPB, EDPS. (2021). EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en

Eiropas Datu aizsardzības kolēģija. (2020). Ieteikumi 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_lv

Eiropas Datu aizsardzības kolēģija. (2020). Pamatnostādnes 04/2020 par atrašanās vietas datu un kontaktu izsekošanas rīku izmantošanu saistībā ar Covid-19 uzliesmojumu. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_lv.pdf

Eiropas Datu aizsardzības uzraudzītājs. (2018). Eiropas Datu aizsardzības uzraudzītāja atzinuma kopsavilkums par priekšlikumu regulai par Savienības pilsoņu personas apliecību un citu dokumentu drošības uzlabošanu. https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_summary_lv_0.pdf

29. panta darba grupa

Article 29 Data Protection Working Party. (2010). Opinion 3/2010 on the principle of accountability. http://www.dataprotection.ro/servlet/ViewDocument?id=654

Article 29 Data Protection Working Party. (2012). Opinion 3/2012 on developments in biometric technologies. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

Article 29 Data Protection Working Party. (2016). Guidelines on Data Protection Officers ('DPOs'). https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

Article 29 Data Protection Working Party. (2016). Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees). https://ec.europa.eu/newsroom/article29/items/640363/en

Article 29 Data Protection Working Party. (2017, as last revised and adopted 2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/612053

Article 29 Data Protection Working Party. (2017). Guidelines on Consent under Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/623051/en

Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"

for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/611236/en

Article 29 Data Protection Working Party. (2017). Guidelines on transparency under Regulation 2016/679. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Eiropas Savienības Kiberdrošības aģentūra (ENISA)

ENISA. (2015). Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. https://www.enisa.europa.eu/publications/big-data-protection

ENISA. (2016). Privacy Enhancing Technologies: Evolution and State of the Art, A Community Approach to PETs Maturity Assessment. https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art

ENISA. (2017). Handbook on Security of Personal Data Processing. https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

Eiropas Savienības Pamattiesību aģentūra

ES Pamattiesību aģentūra, ECT, EP, EDAU. (2018). Rokasgrāmata par Eiropas tiesību aktiem datu aizsardzības jomā. 2018. gada izdevums. https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

FRA. (2018). Handbook on European non-discrimination law. 2018 edition. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-non-discrimination-law-2018_en.pdf

FRA. (2018). Preventing unlawful profiling today and in the future: a guide. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

FRA. (2018). The revised Visa Information System and its fundamental rights implications. https://fra.europa.eu/en/opinion/2018/visa-system

FRA. (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement. https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

FRA. (2020). Coronavirus pandemic in the EU – Fundamental Rights Implications – Bulletin 2. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf

FRA. (2020). Getting the future right. Artificial intelligence and fundamental rights. https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

CITI JURIDISKĀS PRAKSES MATERIĀLI

Latvija

Datu valsts inspekcija. (2018). Apstrādes darbību veidi, attiecībā uz kuriem ir jāveic datu aizsardzības ietekmes novērtējums saskaņā ar VDAR 35. panta 4. punktu. https://www.dvi.gov.lv/lv/media/92/download

VARAM. (2020). Informatīvais ziņojums "Par mākslīgā intelekta risinājumu attīstību". https://www.varam.gov.lv/lv/jauns-informativais-zinojums-par-maksliga-intelekta-risinajumu-attistibu

Apvienotās Karalistes Informācijas komisāra birojs (ICO)

ICO. Data protection by design and by default. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

ICO. Data Protection Impact Assessments (DPIAs). https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

ICO. (2023). Guidance on AI and data protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

ICO. How should we assess security and data minimisation in AI? https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/

ICO. (2019). ICO investigation into how the police use facial recognition technology in public places. https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

Lūgums sniegt prejudiciālu nolēmumu

Lūgums sniegt prejudiciālu nolēmumu, ko 2020. gada 27. maijā iesniedza *Verwaltungsgericht Wiesbaden* (Vācija) – OC/*Bundesrepublik Deutschland*, EST lieta C-148/20, ES OV, C 279/30, 24.08.2020.

Literatūra

Barredo Arrieta, A., Díaz-Rodríguez N., Del Ser J., et al. (2020). Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI. *Information Fusion,* 58, pp. 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Bennett, C. J., Raab, C. D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. 2nd and updated ed. Cambridge, Mass: MIT Press.

Bernal, P. (2015). *Internet Privacy Rights Rights to Protect Autonomy*. Cambridge: Cambridge University Press, http://dx.doi.org/10.1017/CBO9781107337428

van Brakel, R. E. (2021). Rethinking predictive policing: Towards a holistic framework of democratic algorithmic surveillance. In: Schuilenburg, M., Peeters, R. (eds.), *Algorithmic Societies: Power, Knowledge and Technology in the Age of Algorithms*. Routledge, pp. 104–118.

Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81, pp. 77–91, http://proceedings.mlr.press/v81/buolamwini18a.html

Christoffersen, J. and Madsen, M. R. (2011). Introduction: The European Court of Human Rights between Law and Politics. In: Christoffersen, J. and Madsen, M. R. (eds.), *The European Court of Human Rights between Law and Politics*. Oxford: Oxford University Press.

Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the ACM* 31(5), 498-512.

Cohen, J. E. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Stan. L. Rev*., 52, pp. 1373–1438.

Couch, D. L., Robinson, P., and Komesaroff, P. A. (2020). COVID-19 – Extending Surveillance and the Panopticon. *Journal of Bioethical Inquiry*, 17, pp. 809–814. https://doi.org/10.1007/s11673-020-10036-5

Crawford, K., Roel, D., Theodora, D., et al. (2019). AI Now 2019 Report. AI Now Institute. https://ainowinstitute.org/publication/ai-now-2019-report-2

Davies, B., Innes, M., Dawson, A. (2018). An evaluation of South Wales Police's use of Automated Facial Recognition. Cardiff University. https://www.statewatch.org/media/documents/news/2018/nov/uk-south-wales-police-facial-recognition-cardiff-uni-eval-11-18.pdf

van Dijk, P., van Hoof G. J. H., van Rijn, A. B., Zwaak, L. (eds.). (2018). *Theory and Practice of the European Convention on Human Rights*. 5th ed. Cambridge; Antwerp; Portland: Intersentia.

Drechsler, L. (2021). Wanted: LED adequacy decisions How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context. *International Data Privacy Law*, 11(2), pp. 182-195. https://doi.org/10.1093/idpl/ipaa019

Dobber, T., Fathaigh, R. Ó., Zuiderveen Borgesius, F. J. (2019). The regulation of online political micro-targeting in Europe. *Internet Policy Review*, 8(4). https://doi.org/10.14763/2019.4.1440

Donath, J. (2020). Privacy and Public Space. In: *The Social Machine. Design for living online*. https://covid-19.mitpress.mit.edu/pub/8icuynaf

Dignum, V. (2019). *Responsible Artificial Intelligence. How to Develop and Use AI in a Responsible Way*. Springer.

Edwards, L. (ed.). (2019). *Law, Policy, and the Internet*. Oxford, UK; Portland, Orego: Hart Publishing.

Feldman Barrett, L., Adolphs, R., Marsella, S., et al. (2019). Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements. *Psychological Science in the Public Interest*, 20(1), 1–68. https://doi.org/10.1177/1529100619832930

Feldstein, S. (2019). The Global Expansion of AI surveillance. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

Ferguson, A. G. (2017). Big data Surveillance: The Convergence of Big data and Law Enfocement. In: Gray D., Henderson, S. E. (eds.), *The Cambridge Handbook on Surveillance Law*. Cambridge University Press, pp.171–197.

Fjeld, J., Achten, N., Hilligoss, H., et al. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Berkman Klein Center Research Publication No. 2020-1. https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y

Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. *Philosophy & Technology*, 29(4), pp. 307–12. https://doi.org/10.1007/s13347-016-0220-8

Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy and Technology*, 27, pp. 1–3. https://doi.org/10.1007/s13347-014-0157-8

François, C., Allaire, J. J. (2018). *Deep Learning with R*. Shelter Island, NY: Manning Publications Co.

Fussey, P., Murray, D. (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex, Human Rights Centre. https://repository.essex.ac.uk/24946/

Fussey, P., Murray, D. (2020). Policing Uses of Live Facial Recognition in the United Kingdom. In: Kak, A. (ed.), *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute, pp. 78–85. https://ainowinstitute.org/regulatingbiometrics.html

Gonzelez Fuster, G. (2020). Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf

Gstrein, O. J. (2020). Mapping Power and Jurisdiction on the Internet through the Lens of Government-Led Surveillance. *Internet Policy Review*, 9(3). https://doi.org/10.14763/2020.3.1497

Hagendorff, T. (2020). The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds & Machines,* 30, pp. 99–120. https://doi.org/10.1007/s11023-020-09517-8

Hamon, R., Junklewitz, H. and Sanchez, M. J. (2020). Robustness and Explainability of Artificial Intelligence. Publications Office of the European Union, Luxembourg. http://dx.doi.org/10.2760/57493

Harari, Y. N. (2018). *21 Lessons for the 21st Century*. New York: Spiegel & Grau.

Hawkin, S. (2018). *Brief Answers to the Big Questions*. United States: Bantam.

Jobin, A., Ienca, M., Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, pp. 389–399. https://doi.org/10.1038/s42256-019-0088-2

Kindt, E. (2020). A First Attempt at Regulating Biomentric Data in the European Union. In: Kak, A. (ed.). *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute, pp. 62–68. https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions

Kak, A. (ed.). (2020). Regulating Biometrics: Global Approaches and Urgent Questions. AI Now Institute. https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions

Kazim, E., Denny, D. M. T., Koshiyama, A. (2021). AI Auditing and Impact Assessment: According to the UK Information Commissioner's Office. *AI and Ethics*, 1, pp. 301–310. https://doi.org/10.1007/s43681-021-00039-2

Kitchin, R. (2020). Civil Liberties or Public Health, or Civil Liberties and Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19. *Space and Polity*, 24(3), pp. 362–381. https://doi.org/10.1080/13562576.2020.1770587

Kuner, C., Bygrave L. A., Docksey C. (eds.). (2019). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, United Kingdom: Oxford University Press.

Ķinis, U. (2020). Kiberdrošība – tiesiski aizsargājama vērtība. *Jurista Vārds,* 06.10.2020., Nr. 40.

Leslie, D. (2020). Understanding bias in facial recognition technologies: an explainer. The Alan Turing Institute. https://doi.org/10.5281/zenodo.4050457

Lewandowsky, S., Smillie, L., Garcia, D., et al. (2020). Technology and Democracy: Understanding the influence of online technologies on political behaviour and decision-making. Publications Office of the European Union, Luxembourg. https://data.europa.eu/doi/10.2760/709177

Līce, K., Vītola, L. E. (2020). Deklarācija starptautiskajām cilvēktiesību organizācijām par ārkārtējo situāciju Latvijā. *Jurista Vārds*, 14.04.2020., Nr. 15.

Lloyd, I. J. (2020). *Information Technology Law*. (9th ed). Oxford: Oxford University Press.

Manokha, I. (2018). Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance & Society*, 16(2), pp. 219–237. https://doi.org/10.24908/ss.v16i2.8346

Mantelero, A. (2020). Regulating AI within the Human Rights Framework: A Roadmapping Methodology. In: Czech, P., Hesch, L., Lukas, K., Nowak, M., Oberleitner, G. (eds.), *European Yearbook on Human Rights.* Interesentia, pp. 477–502.

Mantelero, A. (2018). AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment. *Computer Law & Security Review*, 34(4), pp. 754–772. https://doi.org/10.1016/j.clsr.2018.05.017

Mantelero, A. (2017). Regulating Big Data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer Law & Security Review,* 33, pp. 584–602.
Marsden, C., Meyer, T. European Parliament. Panel for the Future of Science and Technology. European Science Media-Hub. (2019). Regulating Disinformation with Artificial Intelligence: Effects of Disinformation Initiatives on Freedom of Expression and Media Pluralism. European Union. https://data.europa.eu/doi/10.2861/003689
Mayer-Schonberger V., Cukier K. (2017). *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight*. London: John Murray.
McCrudden, C. (2008). Human Dignity and Judicial Interpretation of Human Rights, *European Journal of International Law*, 19(4), pp. 655–724. https://doi.org/10.1093/ejil/chn043
McDaniel, J. L. M., Pease, K. G. (2021). Introduction. In: McDaniel, J. L. M., Pease, K. G. (eds.), *Predictive Policing and Artificial Intelligence*. Routledge, pp. 1–38.
Mcstay, A. (2020). Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy, Big Data & Society, 7(1). https://doi.org/10.1177/2053951720904386
Michalski, D., Yiu, S. Y., & Malec, C. (2018, February). The impact of age and threshold variation on facial recognition algorithm performance using images of children. In: *2018 International Conference on Biometrics (ICB),* pp. 217–224, IEEE. https://doi.org/10.1109/ICB2018.2018.00041
Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1, pp. 501–507. https://doi.org/10.1038/s42256-019-0114-4
Monahan T., Wood, D. M. Introduction. Surveillance Studies as a Transdisciplinary Endeavor. In: Monahan, T., Wood, D. M. (eds.), (2018). *Surveillance Studies: A Reader*. New York: Oxford University Press.
Monti, A., Wacks, R. (2019). *Protecting Personal Information: The Right to Privacy Reconsidered*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509924882
Moore, P. V. (2020). *Data subjects, digital surveillance, AI and the future of work*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf
Moraes, T. G., Almeida, E. C., de Pereira, J. R. L. (2021). Smile, You Are Being Identified! Risks and Measures for the Use of Facial Recognition in (Semi-)Public Spaces. *AI and Ethics,* 1, pp. 159–172. https://doi.org/10.1007/s43681-020-00014-3
Moreham, N. A. (2006). Privacy in Public Places. *Cambridge Law Journal*, 65(3), pp. 606–635. https://doi.org/10.1017/S0008197306007240
Nemitz, P. (2018). Constitutional Democracy and Technology in the Age of Artificial Intelligence. *Philos. Trans. R. Soc. A-Math. Phys. Eng. Sci.,* 376(2133). https://doi.org/10.1098/RSTA.2018.0089
Nemitz, P. (2018). Profiling the European Citizen: Why today's democracy needs to look harder at the negative potential of new technology than at its positive potential. In: Bayamlioğlu, E., Baraliuc, I., Janssens, L. u. a. (eds.), *Being Profiled: Cogitas Ergo Sum. 10 Years of Profiling the European Citizen.* Amsterdam: Amsterdam University Press, pp. 8–11. https://doi.org/10.2307/j.ctvhrd092.3
Nesterova, I. (2019). Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards. In: Ulrich, G., Ziemele, I. (eds.), *How International Law Works in Times of Crisis*. Oxford University Press, pp. 109–125.

Nijsingh, N., van Bergen, A., Wild, V. (2020). Applying a Precautionary Approach to Mobile Contact Tracing for COVID-19: The Value of Reversibility. *Journal of Bioethical Inquiry*, 17, pp. 823–827. https://doi.org/10.1007/s11673-020-10004-z

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif: Stanford Law Books.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review,* 79(119). https://core.ac.uk/download/pdf/267979739.pdf

Osipova, S. (2020). Bioethics in Correlation with the Principle of Human Dignity. *Journal of the University of Latvia. Law*, 13, pp. 121–136. https://doi.org/10.22364/jull.13.07

Pati, R. (2009). *Due Process and International Terrorism*. Leiden, Boston: Nijhoff.

Pauwels, E. (2020). Artificial Intelligence and data capture technologies in violence and conflict prevention. https://www.globalcenter.org/wp-content/uploads/2020/10/GCCS_AIData_PB_H.pdf

Perry, W. L. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND.

Rainey, B., McCormick, P., Ovey, C. (2021). *Jacobs, White, and Ovey: The European Convention on Human Rights*. Oxford University Press.

Regan, P. M. (2009). *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill, NC: The University of North Carolina Press.

Reisman, D., Schultz, J., Crawford, K., Whittaker, M. (2018). Algorithmic Impact Assessments Report: A Practical Framework for Public Agency Accountability. https://ainowinstitute.org/publication/algorithmic-impact-assessments-report-2

Rouhiainen, L. (2019). *Artificial Intelligence: 101 Things You Must Know Today about Our Future*, CreateSpace Independent Publishing Platform.

Rudgard, S. (2018). Origins and Historical Context of Data Protection Law. In: Ustaran, E., Lovells, H. (eds.), *European Data Protection. Law and Practice.* International Association of Privacy Professionals (IAPP).

Russel, S. J., Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*. Pearson Series in Artificial Intelligence. Hoboken: Pearson.

Ryan, M., Stahl, B. C. (2020). Artificial Intelligence Ethics Guidelines for Developers and Users: Clarifying Their Content and Normative Implications, *Journal of Information, Communication and Ethics in Society,* 19(1). https://doi.org/10.1108/JICES-12-2019-0138

Sartor, G., Lagioia, F. (2020) The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*.* European Parliament. http://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

Schneier, B. (2016). *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World.* New York, London: W. W. Norton & Company.

Solove, D. J. (2009). *Understanding Privacy*. Cambridge, Massachusetts London, England: Harvard University Press.

Spadaro, A. (2020). COVID-19: Testing the Limits of Human Rights. *European Journal of Risk Regulation*, 11(2), pp. 317–325. https://doi.org/10.1017/err.2020.27

Stanley, J., Granick, J. S. (2020). The Limits of Location Tracking in an Epidemic. ACLU. https://www.aclu.org/wp-content/uploads/legal-documents/limits_of_location_tracking_in_an_epidemic.pdf

Susser, D., Roessler, B., Nissenbaum, H. (2019). Technology, Autonomy, and Manipulation. *Internet Policy Review,* 8(2). https://doi.org/10.14763/2019.2.1410

Taylor, L., Floridi L., van der Sloot B. (eds.). (2017). *Group Privacy: New Challenges of Data Technologies*. Cham: Springer International Publishing, https://doi.org/10.1007/978-3-319-46608-8

Taylor, L., van der Sloot, B., and Floridi, L. (2017). Conclusion: What Do We Know About Group Privacy? In: Taylor, L, Floridi, L., van der Sloot, B. (eds.), *Group Privacy*, pp. 225–37. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8_12

Thomson, J. J. (1975). The Right to Privacy. *Philosophy and Public Affairs*, 4(4), pp. 295–314.

Tokson, M. (2020). The Emerging Principles of Fourth Amendment Privacy. *The George Washington Law Review*, 88(1). https://www.gwlr.org/wp-content/uploads/2020/05/88-Geo.-Wash.-L.-Rev.-1.pdf

Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind 49*, pp. 433–460. https://www.csee.umbc.edu/courses/471/papers/turing.pdf

Tzanou, M. (2013). Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 3(2), https://doi.org/10.1093/idpl/ipt004

Tzanou, M. (2019). *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*. Oxford: Hart Publishing.

Vargo, D., Zhu, L., Benwell, B., Yan, Z. (2021). Digital Technology Use during COVID-19 Pandemic: A Rapid Review. *Human Behavior and Emerging Technologies,* 3(1), pp. 13–24. https://doi.org/10.1002/hbe2.242

Véliz, C. (2021). *Privacy Is Power: Why and How You Should Take Back Control of Your Data.* Bantam Press.

Waldron, J. (2013). Is Dignity the Foundation of Human Rights? *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.2196074

Warren, S., Brandais, L. D. (1890). The right to privacy. *Harward Law Review*, 4, pp. 193–220. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Weissman, D. (2018). Autonomy and Free Will: Autonomy and Free Will. *Metaphilosophy*, 49(5), pp. 609–645. https://doi.org/10.1111/meta.12333

Westin, A. F. (1967). *Privacy and Freedom*, New York: Atheneum.

Whitelaw, S., Mamas, A., Topol, E., van Spall, H. G. C. (2020). Applications of Digital Technology in COVID-19 Pandemic Planning and Response. *The Lancet Digital Health,* 2(8), https://doi.org/10.1016/S2589-7500(20)30142-4

Wilson, D. (2018). Algorithmic patrol: the futures of predictive policing. In: Zavrsnik, A. (ed.), *Big Data, Crime and Social Control. Routledge Frontiers of Criminal Justice*. Routledge, London.

Yeung, K., Howes, A., Pogrebna, G. (2020). AI Governance by Human Rights-Centered Design, Deliberation, and Oversight: An End to Ethics Washing. In: Dubber, M. D., Pasquale, F., and Das, S. (eds.), *The Oxford Handbook of Ethics of AI*, pp. 75–106. Oxford University Press, https://doi.org/10.1093/oxfordhb/9780190067397.013.5

Zuboff, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the new Frontier of Power.* Profile Books.

CITI MATERIĀLI (ZIŅAS, INFORMĀCIJA UN CITI INTERNETA RESURSI)

Access Now. (2018). Human rights in the age of artificial intelligence. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

Ackerman, S., Rushe, D. (3 February, 2014). The Microsoft, Facebook, Google and Yahoo release US surveillance requests. *The Guardian*. http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests

Andrews, E. L. (11 June, 2020). Governments Aren't Yet Serious About AI's Risk to Human Rights. *Stanford University Human-Centered Artificial Intelligence.* https://hai.stanford.edu/news/governments-arent-yet-serious-about-ais-risk-human-rights

Aris, B. (25 September, 2020). Belarus IT specialists develope software to identify OMON officers waring masks. *bne IntelliNews.* https://www.intellinews.com/belarus-it-specialists-develop-software-to-identify-omon-officers-wearing-masks-192747/

Article 19. (2021). Emotional Entanglement: China's emotion recognition market and its implications for human rights. https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf

Aystin, D. (16 April, 2021). Here is Your 2021 Internet Minute Infographic!: eDiscovery Trends. *eDiscoveryToday.* https://ediscoverytoday.com/2021/04/16/here-is-your-2021-internet-minute-infographic-ediscovery-trends/

Ball, S. (24 March, 2020). 100,000 cameras: Moscow uses facial recognition to enforce quarantine. *France24*. https://www.france24.com/en/20200324-100-000-cameras-moscow-uses-facial-recognition-to-enforce-quarantine

Booth, R. (3 July, 2019). Police face calls to end use of facial recognition software. *The Guardian*. https://www.theguardian.com/technology/2019/jul/03/police-face-calls-to-end-use-of-facial-recognition-software

Burgess, M. (4 September, 2019). UK police can use controversial facial recognition tech, court rules. *WIRED.* https://www.wired.co.uk/article/police-facial-recognition-south-wales-court-decision

Busvine, D. (7 April, 2020). Germany launches smartwatch app to monitor coronavirus spread. *Reuters.* https://www.reuters.com/article/us-health-coronavirus-germany-tech-idUSKBN21P1SS

Buttarelli, G. (19 October, 2018). The urgent case for a new ePrivacy law. *EDPS*. https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en

Countries are using apps and data networks to keep tabs on the pandemic. (26 March, 2020). *The Economist.* https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic

European Citizens' Initiative. Civil society initiative for a ban on biometric mass surveillance practices. https://reclaimyourface.eu

CNIL. (29 Octobre, 2019). Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position. https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

CNIL. (2019). The open source PIA software helps to carry out data protection impact assessment. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

CNIL. (9 Octobre, 2020). Reconnaissance faciale dans les aéroports: quels enjeux et quels grands principes à respecter? https://www.cnil.fr/fr/reconnaissance-faciale-dans-les-aeroports-quels-enjeux-et-quels-grands-principes-respecter

Coalition Letter Requests Federal Moratorium on the Use of Facial Recognition Technology. (16 February, 2021). *Freedom House.* https://freedomhouse.org/article/coalition-letter-requests-federal-moratorium-use-facial-recognition-technology

Council of Europe. Chart of signatures and ratifications of Treaty 108. Status as of 12/06/2021. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures

Council of Europe. Chart of signatures and ratifications of Treaty 223. Status as of 12/06/2021. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures?p_auth=iyy2ZbpX

Council of Europe. (2018). Mass surveillance. https://rm.coe.int/factsheet-on-mass-surveillance-june2018-docx/16808b3dd8

Council of Europe. Recommendations, resolutions and guidelines. https://www.coe.int/en/web/cdcj/recommendations-resolutions-guidelines

Dearden, L. (7 May, 2019). Facial recognition wrongly identifies public as potential criminals 96 % of time, figures reveal. *Independent.* https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html

DeCew, J. (2018). Privacy. In: Zalta, E. N. (ed.), *The Stanford Encyclopedia of Philosophy.* https://plato.stanford.edu/archives/spr2018/entries/privacy/

Deegan, G. (11 September, 2018). Facial imaging software detects 28 cases of welfare fraud in 2018. *The Irish Times.* https://www.irishtimes.com/news/crime-and-law/facial-imaging-software-detects-28-cases-of-welfare-fraud-in-2018-1.3626076

Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown. (16 April, 2020). *University of Oxford.* https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

Doffman, Z. (14 August, 2019). New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report. *Forbes.* https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#76f9901046c6

Dutch police facial recognition database includes 1.3 million people. (22 July, 2019). *DutchNews.nl.* https://www.dutchnews.nl/news/2019/07/dutch-police-facial-recognition-database-includes-1-3-million-people/

EDPB. (22 August, 2019). Facial recognition in school renders Sweden's first GDPR fine. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

EDPB. (21 February, 2021). Swedish DPA: Police unlawfully used facial recognition app. https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_lv

EDPS. (23 April, 2021). Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary. https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en

EDRi. EU's AI law needs major changes to prevent discrimination and mass surveillance. https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/

EDRi. (17 February, 2021). New ECI calls Europeans to stand together for a future free from harmful biometric mass surveillance. https://edri.org/our-work/new-eci-ban-biometric-mass-surveillance/

EDRi. (12 January, 2021). Re: Open letter: Civil society call for the introduction of red lines in the upcoming European Commission proposal on Artificial Intelligence. https://edri.org/wp-content/uploads/2021/01/EDRi-open-letter-AI-red-lines.pdf

E-health Network. (2020). Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States. https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19_apps_en.pdf

European Commission. (2020). Mobile applications to support contact tracing in the EU's fight against COVID-19. Progress reporting June 2020. https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf

Gallagher, R., Jona, L. (26 July, 2019). We tested Europe's new lie detector for travellers – and immediately triggered a false positive. *The Intercept.* https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/

Gellman, B., Poitras, L. (7 June, 2013). Washington Post: U.S., British intelligence mining data from nine US Internet companies in broad secret program. *Government Accountability Project.* https://whistleblower.org/in-the-news/washington-post-us-british-intelligence-mining-data-nine-us-internet-companies-broad/

Glaser, A. (12 February, 2014). Academics and Researchers Against Mass Surveillance. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2014/02/academics-and-researchers-against-mass-surveillance

Goh, B. (26 February, 2020). China rolls out fresh data collection campaign to combat coronavirus. *Reuters.* https://www.reuters.com/article/us-china-health-data-collection/china-rolls-out-fresh-data-collection-campaign-to-combat-coronavirus-idUSKCN20K0LW

Greene, J. (11 June, 2020). Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM. *The Washington Post.* https://www-washingtonpost-com.cdn.ampproject.org/c/s/www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/?outputType=amp

Google CEO backs GDPR, says privacy should not be a luxury. (22 January, 2020). *The Institute of Engineering & Technology.* https://eandt.theiet.org/content/articles/2020/01/google-ceo-backs-gdpr-says-privacy-should-not-be-a-luxury/

Government of Canada. Algorithmic Impact Assessment. https://canada-ca.github.io/aia-eia-js/

Greenwald, G., MacAskill, E. (7 June, 2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian.* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Halbfinger, D. M., Kershner, I., Bergman, R. (18 March, 2020). To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data. *The New York Times.* https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html

Harari, Y. N. (14 September, 2018). Yuval Noah Harari: the myth of freedom. *The Guardian.* https://www.theguardian.com/books/2018/sep/14/yuval-noah-harari-the-new-threat-to-liberal-democracy

Harari, Y. N. (2020). Yuval Noah Harari: "Every crisis is also an opportunity." *UNESCO Courier*, 2020-3. https://en.unesco.org/courier/2020-3/yuval-noah-harari-every-crisis-also-opportunity

Harari, Y. N. (20 March, 2020). Yuval Noah Harari: the world after coronavirus. *Financial Times.* https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Hardesty, L. (11 February, 2018). Study finds gender and skin-type bias in commercial artificial-intelligence systems. *Massachusetts Institute of Technology.* https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

Hendry, J. (19 April, 2020). WA to electronically track COVID-19 patients who defy isolation orders. *iTnews.* https://www.itnews.com.au/news/wa-to-electronically-track-covid-19-patients-who-defy-isolation-orders-546224

Hidvegi, F., Leufer, D., Massé, E. (17 February, 2021). The EU should regulate AI on the basis of rights, not risks. *Access Now*. https://www.accessnow.org/eu-regulation-ai-risk-based-approach/

Holmes, A. (12 August, 2020). Instagram could face up to $500 billion in fines in class-action lawsuit alleging it illegally harvested biometric data. *Insider.* https://www.businessinsider.com/instagram-facing-500-billion-in-fines-in-facial-recognition-lawsuit-2020-8

van den Hoven, J., Blaauw, M., Pieters, W., Warnier, M. (2014, 2019 ed.). Privacy and Information Technology. In: Zalta, E. N. (ed.), The Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/archives/sum2020/entries/it-privacy/

IEEE. (2019). Ethically Aligned Design. First Edition: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf?utm_medium=undefined&utm_source=undefined&utm_campaign=undefined&utm_content=undefined&utm_term=undefined

Ilves, I. (16 June, 2020). Why are Google and Apple dictating how European democracies fight coronavirus? *The Guardian.* https://www.theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-european-democracies-coronavirus

Ilyushina, M. (14 April, 2020). Moscow rolls out digital tracking to enforce lockdown. Critics dub it a 'cyber Gulag'. *CNN*. https://edition.cnn.com/2020/04/14/world/moscow-cyber-tracking-qr-code-intl/index.html

Jennings, R. (11 December, 2009). Google CEO: if you want privacy, do you have something to hide? *Computerworld.* https://www.computerworld.com/article/2468308/google-ceo--if-you-want-privacy--do-you-have-something-to-hide-.html

Kobie, N. (7. June, 2019) The Complicated truth about China's social credit system. *WIRED.* https://www.wired.co.uk/article/china-social-credit-system-explained

Kallingal, M. (3 April, 2020). Ankle monitors ordered for Louisville, Kentucky residents exposed to Covid-19 who refuse to stay home. *CNN*. https://edition.cnn.com/2020/04/03/us/kentucky-coronavirus-residents-ankle-monitors-trnd/index.html

Karen, H. (June 12, 2020). The two-year fight to stop Amazon from selling face recognition to the police. *MIT Technology Review.* https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/

Kayali, L. (29 October, 2019). French privacy watchdog says facial recognition trial in high schools is illegal. *POLITICO.* https://www.politico.eu/article/french-privacy-watchdog-says-facial-recognition-trial-in-high-schools-is-illegal-privacy/

Kayser-Bril, N. (18 June, 2020). At least 11 police forces use face recognition in the EU, Algorithm Watch reveals. *Algorithm Watch.* https://algorithmwatch.org/en/face-recognition-police-europe/

Kelion, L. (1 September, 2020). Coronavirus: Apple iPhones can contact-trace without Covid app. *BBC News.* https://www.bbc.com/news/technology-53987928

Kelly, E. (21 January, 2020). EU makes move to ban use of facial recognition systems. *Science|Business.* https://sciencebusiness.net/news/eu-makes-move-ban-use-facial-recognition-systems

Kharpal, A. (28 January, 2020). Big Tech's calls for more regulation offers a chance for them to increase their power. *CNBC.* https://www.cnbc.com/2020/01/28/big-techs-calls-for-ai-regulation-could-lead-to-more-power.html

Kučić, L. J. (7 July, 2020). Slovenian police acquires automated tools first, legalizes them later. *Algorithm Watch*. https://algorithmwatch.org/en/slovenia-police-face-recognition/

Kuner, C. (17 July, 2020). The Schrems II judgment of the Court of Justice and the future of data transfer regulation. *European Law Blog.* https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

Lyons, K. (13 February, 2021). Minneapolis prohibits use of facial recognition software by its police department. *The Verge*. https://www.theverge.com/2021/2/13/22281523/minneapolis-prohibits-facial-recognition-software-police-privacy

Manancourt, V. (15 June, 2020). Norway suspends contact-tracing app over privacy concerns. *POLITICO.* https://www.politico.eu/article/norway-suspends-contact-tracing-app-over-privacy-concerns/

McDonald, T. (25 September, 2020). Singapore in world first for facial verification. *BBC News.* https://www.bbc.com/news/business-54266602

Mohan, M. (12 September, 2020). More than 3,500 electronic wristband devices issued to travellers serving stay-home notices: ICA. *CNA.* https://www.channelnewsasia.com/news/singapore/electronic-wristband-devices-stay-home-notice-ica-covid-19-13105390

Moyer, E. (27 February, 2021). Facebook privacy lawsuit over facial recognition leads to $650M settlement. *Reuters.* https://www.reuters.com/article/us-facebook-privacy-lawsuit-idUSKCN25G08M

Musil, S. (14 July, 2020). Amazon, Google, Microsoft sued over photos in facial recognition database. *CNET.* https://www.cnet.com/news/amazon-google-and-microsoft-sued-over-photos-in-facial-recognition-database/

Naughton, J. (20 January, 2019). 'The goal is to automate us': welcome to the age of surveillance capitalism. *The Guardian.* https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

Nickelsburg, M. (21 January, 2020). Microsoft President Brad Smith calls for AI regulation at Davos. *GeekWire.* https://www.geekwire.com/2020/microsoft-president-brad-smith-calls-ai-regulation-davos/

O'Donoghou C., O'Brien S. (17 August, 2020). Face-off part 2: UK Court of Appeal finds deficiencies in use of automated facial recognition technology. *Technology Law Dispatch.* https://www.technologylawdispatch.com/2020/08/in-the-courts/face-off-part-2-uk-court-of-appeal-finds-deficiencies-in-use-of-automated-facial-recognition-technology

OECD. AI Policy Observatory. https://oecd.ai

Open letter to EU Member States. (11 October, 2019). *EDRi.* https://edri.org/files/eprivacy/ePrivacy_NGO_letter_20191011.pdf

Our legal action against the use of facial recognition by the french police. (21 September, 2020). La *Quadrature du Net.* https://www.laquadrature.net/en/2020/09/21/our-legal-action-against-the-use-of-facial-recognition-by-the-french-police/

Paresh, D., Jeffrey, D. (19 April, 2021). U.S. banks deploy AI to monitor customers, workers amid tech backlash. *Reuters.* https://www.reuters.com/technology/us-banks-deploy-ai-monitor-customers-workers-amid-tech-backlash-2021-04-19/

Peters, J. (9 September 2020). Portland passes strongest facial recognition ban in the US. *The Verge*. https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology

Pugh, A. (28 May, 2020). Lithuanian contact tracing app suspended. *Global Data Review.* https://globaldatareview.com/coronavirus/lithuanian-contact-tracing-app-suspended

Ravani, S. (17 July, 2019). Oakland bans use of facial recognition technology, citing bias concerns. *San Francisco Chronicle.* https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php

Rahman, M. (25 February, 2021). Here are the countries using Google and Apple's COVID-19 Contact Tracing API. *XDA Developers.* https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/

Roussi, A. (18 November, 2020). Resisting the rise of facial recognition. *Nature.* https://www.nature.com/articles/d41586-020-03188-2

Satversmes tiesa. (2020. gada 2. decembris). Satversmes tiesas priekšsēdētāja Sanita Osipova akcentē cilvēka cieņas un iecietības nozīmi pamattiesību īstenošanā. *Jurista Vārds.* https://juristavards.lv/zinas/277771-satversmes-tiesas-priekssedetaja-sanita-osipova-akcente-cilveka-cienas-un-iecietibas-nozimi-pamattiesibu-istenosana/

Serbia: Violent police crackdown against COVID-19 lockdown protesters must stop. (9 July, 2020). *Amnesty International.* https://www.amnesty.org/en/latest/news/2020/07/serbia-violent-police-crackdown-against-covid-19-lockdown-protesters-must-stop/

SHARE Foundation, Hermes Center, Bits of Freedom, ARTICLE19, Homo Digitalis and EDRi. (12 November, 2020). Campaign "Reclaim Your Face" calls for a Ban on Biometric Mass Surveillance. *EDRi.* https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/

Sherman, J. (28 January, 2020). Oh Sure, Big Tech Wants Regulation—on Its Own Terms. *WIRED*. https://www.wired.com/story/opinion-oh-sure-big-tech-wants-regulationon-its-own-terms/

Singer, N., Sang-Hun, C. (23 Mach, 2020). As Coronavirus Surveillance Escalates, Personal Privacy Plummets. *The New York Times*. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

Social Science Research Council. (2021). Surveillance and the 'New Normal' of Covid-19: Public Health, Data, and Justice. https://covid19research.ssrc.org/public-health-surveillance-and-human-rights-network/report/

Spundiņa, L. (1. oktobris, 2020). Datu valsts inspekcija neatbalsta sejas atpazīšanas video-novērošanas iekārtas. *LSM.lv.* https://www.lsm.lv/raksts/zinas/latvija/datu-valsts-inspekcija-neatbalsta-sejas-atpazisanas-videonoverosanas-iekartas.a376399/

Statement on an agreement reached between Facebook and the ICO. (30 October, 2019). *WIRED*. https://www.wired-gov.net/wg/news.nsf/articles/Statement+on+an+agreement+reached+between+Facebook+and+the+ICO+30102019151000?open

Statista. (2019). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Statt, N. (28 May 2020). ACLU sues facial recognition firm Clearview AI, calling it a 'nightmare scenario' for privacy. *The Verge.* https://www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws

Sterling, B. (17 January, 2014). Academics Against Mass Surveillance. *WIRED*. https://www.wired.com/2014/01/academics-mass-surveillance/

Stolton, S. (8 February, 2021). Commission under pressure in EU court over 'lie detector tech'. *EURACTIV.* https://www.euractiv.com/section/digital/news/aommission-under-pressure-over-lie-detector-tech-in-eu-courts/

Stolton, S. (10 November 2020). EU to restrict sale of cyber-surveillance goods to repressive regimes. *EURACTIV.* https://www.euractiv.com/section/digital/news/eu-to-restrict-sale-of-cyber-surveillance-goods-to-repressive-regimes/

Stone, M., Bartz, D. (8 January, 2021). Some U.S. Capitol rioters fired after internet detectives identify them. *Reuters.* https://www.reuters.com/article/us-usa-election-protests-fallout-idUSKBN29C36M

Swisher, K. (27 November, 2020). Amazon wants to get even closer. Skintight. *The New York Times.* https://www.nytimes.com/2020/11/27/opinion/amazon-halo-surveillance.html
Timberg, C., Harwell, D. (19 March 2020). Government efforts to track virus through phone location data complicated by privacy concerns. *The Washington Post.* https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/
The Facebook CEO Chellenges the social norm of Privacy. (12 January, 2010). *Reuters.* https://www.reuters.com/article/urnidgns852573c400693880002576a80069db04/facebook-ceo-challenges-the-social-norm-of-privacy-idUS174222527820100112
The Global Partnership on Artificial Intelligence. https://gpai.ai
Ulmer, A., Siddiqui, Z. (17 February, 2020). India's use of facial recognition tech during protests causes stir. *Reuters.* https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ
UN News. (5 November, 2018). 'Warp speed' technology must be 'force for good' UN chief tells web leaders. https://news.un.org/en/story/2018/11/1024982
UNCTAD. Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
Vinocur, N. (30 October, 2020). French politicians urge deployment of surveillance technology after series of attacks. *POLITICO*. https://www.politico.eu/article/french-politicians-urge-deployment-of-surveillance-technology-after-series-of-attacks/
Wakefield, J. (26 May, 2021). AI emotion-detection software tested on Uyghurs. *BBC News.* https://www.bbc.com/news/technology-57101248
WHO. (13 March, 2020). WHO Director-General's opening remarks at the media briefing on COVID-19 – 13 March 2020. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-mission-briefing-on-covid-19---13-march-2020
Wiewiórowski, W. (30 April, 2020). Carrying the torch in times of darkness. *EDPS.* https://edps.europa.eu/press-publications/press-news/blog/carrying-torch-times-darkness_en
Wong, Q. (27 March, 2019). Why facial recognition's racial bias problem is so hard to track. *CNET.* https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack/
Ziemele, I. (31 January, 2020). Opening of the Judicial Year Seminar. The European Convention on Human Rights: Living Instrument at 70 – Science and Technology. https://echr.coe.int/Documents/Speech_20200131_Ziemele_JY_ENG.pdf

Jēdzienu rādītājs

Irēna Barkāne
Cilvēktiesību nozīme mākslīgā intelekta laikmetā
Privātums, datu aizsardzība un regulējums
masveida novērošanas novēršanai

LU Akadēmiskais apgāds
Aspazijas bulvāris 5–132, Rīga, LV-1050, Latvija
www.apgads.lu.lv
Interneta grāmatnīca: gramatas.lu.lv

Iespiests SIA "Jelgavas tipogrāfija"

Cilvēktiesību nozīme mākslīgā intelekta laikmetā

Privātums, datu aizsardzība un regulējums masveida novērošanas novēršanai

Irēna Barkāne

Cilvēktiesību nozīme mākslīgā intelekta laikmetā

Privātums, datu aizsardzība un regulējums masveida novērošanas novēršanai

LU Akadēmiskais apgāds

UDK 34:004.8
Ba653

Irēna Barkāne. *Cilvēktiesību nozīme mākslīgā intelekta laikmetā. Privātums, datu aizsardzība un regulējums masveida novērošanas novēršanai.* Rīga: LU Akadēmiskais apgāds, 2023. 328 lpp.

Monogrāfija sagatavota un izdota ar Eiropas Reģionālā attīstības fonda darbības programmas "Izaugsme un nodarbinātība" specifiskā atbalsta mērķa 1.1.1.2. pasākuma "Pēcdoktorantūras pētniecības atbalsts" atbalstu projektā Nr. 1.1.1.2./VIAA1/1/16/196 "Taisnīgs līdzsvars starp privātumu un drošību kibertelpā: stingru datu aizsardzības standartu izveide Eiropā".

Monogrāfija atbalstīta izdošanai ar Latvijas Universitātes Humanitāro un sociālo zinātņu padomes 2021. gada 12. jūlija sēdes lēmumu (protokols Nr. 8).

LATVIJAS UNIVERSITĀTE

Recenzenti:

asociētais profesors *Dr*. Alesandro Mantelero (*Alessandro Mantelero*),
Turīnas Politehniskais institūts (*Polytechnic University of Turin*), Itālija;

asociētais profesors *Dr. iur*. Uldis Ķinis, Rīgas Stradiņa universitāte, Latvija

Latviešu valodas korektores Agita Kazakeviča un Ieva Zarāne

Angļu valodas korektori Andra Damberga,
Kristofers Godards (*Christopher Goddard*)

Maketu un vāka dizainu veidojusi Baiba Lazdiņa

ISBN 978-9934-36-097-8
ISBN 978-9934-36-098-5 (PDF)
https://doi.org/10.22364/cnmil.23

Monogrāfija veltīta mākslīgā intelekta tiesiskajiem un cilvēktiesību jautājumiem. Mākslīgais intelekts var sniegt ievērojamu labumu daudzās jomās, bet tas rada arī jaunus apdraudējumus. Viens no būtiskiem mākslīgā intelekta radītajiem izaicinājumiem ir mākslīgā intelekta novērošanas tehnoloģijas. Tās var aizskart cilvēka cieņu, tiesības uz privātumu un datu aizsardzību, diskriminācijas aizlieguma principu un pulcēšanās brīvību, kā arī apdraudēt tiesiskumu un demokrātiju. Gan Eiropā, gan visā pasaulē valstis, atsaucoties uz nacionālās drošības un sabiedrības drošības aizsardzības interesēm, strauji ievieš dažāda veida mākslīgā intelekta novērošanas tehnoloģijas. Sejas atpazīšanas tehnoloģijas, emociju uztveršanas tehnoloģijas, noziedzības prognozēšanas un automatizētu lēmumu pieņemšanas sistēmas ir radījušas plašas diskusijas par to ētisko, tiesisko un sociālo ietekmi un nepieciešamību ierobežot un aizliegt to izmantošanu. Esošais tiesiskais regulējums, īpaši cilvēktiesības un datu aizsardzības tiesības, jau šobrīd regulē mākslīgā intelekta tehnoloģijas, kā arī tiek izstrādāts jauns mākslīgā intelekta regulējums, ko ir nepieciešams izvērtēt.

Grāmatā vispirms ir apskatīta mākslīgā intelekta novērošanas tehnoloģiju izmantošana tiesībaizsardzības jomā Eiropā un pasaulē un izvērtēta to ietekme uz cilvēktiesībām. Pēc tam tajā ir aplūkotas tiesības uz privātumu, datu aizsardzības tiesības, kā arī mākslīgā intelekta regulējuma attīstība starptautiskā un Eiropas līmenī. Grāmatas turpinājumā ir analizēti Eiropas Cilvēktiesību tiesas un Eiropas Savienības Tiesas praksē izstrādātie nosacījumi tiesību uz privātumu un datu aizsardzību ierobežošanai un Eiropas datu aizsardzības prasības, kas piemērojamas mākslīgā intelekta novērošanas pasākumiem. Nobeigumā ir sniegtas rekomendācijas mākslīgā intelekta tiesiskā regulējuma un politikas tālākai attīstībai, kas būtu balstīta cilvēktiesībās un noteiktu efektīvas aizsardzības garantijas un mehānismus, kā arī ierobežojumus un aizliegumus, lai nodrošinātu mākslīgā intelekta tehnoloģiju atbildīgu un uzticamu izmantošanu un novērstu to radīto apdraudējumu un masveida novērošanu.

Grāmata būs noderīga mācībspēkiem un zinātniekiem, studentiem, tiesību piemērotājiem un digitālās politikas veidotājiem, iestādēm un uzņēmumiem, kas izstrādā, ievieš un izmanto mākslīgā intelekta tehnoloģijas, kā arī ikvienam lasītājam, kuram ir interese par cilvēktiesībām, datu aizsardzības tiesībām, Eiropas Savienības tiesībām, mākslīgā intelekta un jauno tehnoloģiju regulējuma attīstību.

Saturs

6. DAĻA

7. DAĻA

SUMMARY

IZMANTOTIE SAĪSINĀJUMI

AHEG	*UNESCO Ad Hoc Expert Group (AHEG) for the preparation of a draft text of a Recommendation on the Ethics of Artificial Intelligence* – angļu val.; UNESCO Starptautiskā *ad hoc* ekspertu grupa Rekomendācijas par mākslīgā intelekta ētiku izstrādei
AI HLEG	*High-Level Expert Group on Artificial Intelligence set up by the European Commission* – angļu val.; Eiropas Komisijas izveidota augsta līmeņa ekspertu grupa mākslīgā intelekta jautājumu risināšanai
ANO	Apvienoto Nāciju Organizācija
CAHAI	*Ad hoc Committee on Artificial Intelligence of the Council of Europe* – angļu val.; Eiropas Padomes Mākslīgā intelekta *ad hoc* komiteja
CCTV	*Closed-circuit television* – angļu val.; videonovērošanas kameras/ sistēma
CNIL	*Commission Nationale de l'Informatique et des Libertés* – franču val.; Francijas datu aizsardzības iestāde
Direktīva 95/46/EK	Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti
ECT	Eiropas Cilvēktiesību tiesa
ECTK	Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija
EDRi	*European Digital Rights* – angļu val.; Eiropas Digitālo tiesību asociācija
Eiropols	Eiropas Savienības Aģentūra tiesībaizsardzības sadarbībai
ENISA	Eiropas Savienības Kiberdrošības aģentūra
E-privātuma direktīva	Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju)
E-privātuma regulas priekšlikums	Eiropas Komisijas priekšlikums Eiropas Parlamenta un Padomes regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula)
EST	Eiropas Savienības Tiesa
FPDAL	Fizisko personu datu apstrādes likums
FRA	*European Union Agency for Fundamental Rights* – angļu val.; Eiropas Savienības Pamattiesību aģentūra
Harta	Eiropas Savienības Pamattiesību harta

ICO	*The Information Commissioner's Office* – angļu val.; Apvienotās Karalistes Informācijas komisāra birojs
Konvencija 108	Eiropas Padomes Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi
Konvencija 108+	Eiropas Padomes modernizētā Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi
LES	Līgums par Eiropas Savienību
LESD	Līgums par Eiropas Savienības darbību
MI akta priekšlikums	Eiropas Komisijas priekšlikums Eiropas Parlamenta un Padomes regulai, kas nosaka saskaņotas normas mākslīgā intelekta jomā (Mākslīgā intelekta akts) un groza dažus Savienības leģislatīvos aktus
MI ētikas vadlīnijas	AI HLEG Ētikas vadlīnijas uzticamam mākslīgajam intelektam
NIS direktīva	Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā
NSA	*National Security Agency* – angļu val.; ASV Nacionālās drošības aģentūra
OECD	*Organisation for Economic Co-operation and Development* – angļu val.; Ekonomiskās sadarbības un attīstības organizācija
OHCHR	*The Office of the United Nations High Commissioner for Human Rights* – angļu val.; Apvienoto Nāciju Organizācijas Augstā cilvēktiesību komisāra birojs
Policijas direktīva	Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI
Satversme	Latvijas Republikas Satversme
SPPPT	Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām
UNESCO	*United Nations Educational, Scientific and Cultural Organisation* – angļu val.; Apvienoto Nāciju Izglītības, zinātnes un kultūras organizācija
UNICEF	*The United Nations International Children's Emergency Fund* – angļu. val.; ANO Bērnu fonds
UNICRI	*United Nations Interregional Crime and Justice Research Institute* – angļu val.; ANO Starpreģionālās noziedzības un tieslietu pētniecības institūts
VDAR	Vispārīgā datu aizsardzības regula

IEVADS

Mākslīgā intelekta attīstība notiek ļoti strauji. Tas lielā mērā pārveido sabiedrību un var sniegt nozīmīgus ieguvumus daudzās jomās, to skaitā zinātnes, izglītības, transporta, nodarbinātības, kultūras, veselības, tiesībaizsardzības un drošības jomā, bet vienlaikus tas rada arī daudz jaunu izaicinājumu. Viens no lielākajiem izaicinājumiem ir mākslīgā intelekta novērošanas tehnoloģijas, kas rada būtisku apdraudējumu cilvēktiesībām, tiesiskumam un demokrātijai.

Arvien vairāk valstu visā pasaulē izmanto mākslīgā intelekta novērošanas tehnoloģijas – sejas atpazīšanas sistēmas, automatizētu lēmumu pieņemšanas un prognozēšanas sistēmas, automatizētas robežkontroles sistēmas utt.[1] Visplašākās diskusijas, kā arī kritiku ir radījušas sejas atpazīšanas tehnoloģijas, to izmantošana strauji pieaug gan valsts, gan privātā sektorā. Daudzās Eiropas valstīs, piemēram, Lielbritānijā, Francijā, Vācijā, Spānijā, Nīderlandē, tās arvien vairāk izmanto policija un citas tiesībaizsardzības iestādes, bieži vien slepenā un nekontrolētā veidā. Tās ievieš arī citas publiskas iestādes un privātie uzņēmumi, lai veiktu novērošanu, piemēram, darbā, skolās, lielveikalos, lidostās, sporta pasākumos utt.

Starptautiskās organizācijas, valstu likumdevēji, uzraudzības iestādes, nevalstiskās organizācijas, cilvēktiesību aizstāvji un zinātnieki arvien vairāk uzsver nepieciešamību regulēt vai pat aizliegt šo tehnoloģiju izmantošanu. 2019. gadā Sanfrancisko bija pirmā Amerikas Savienoto Valstu pilsēta, kas aizliedza šīs tehnoloģijas izmantot policijas un valsts iestādēm. Drīz arī citas ASV pilsētas, to skaitā Oklenda, Bostona, Mineapolisa, pieņēma līdzīgus noteikumus, ņemot vērā, ka daudzos gadījumus šīs tehnoloģijas atspoguļo aizspriedumus, piemēram, pēc rases, vecuma un etniskās piederības, un ir diskriminējošas.[2]

Arī Eiropā tiek plaši diskutēts, kā regulēt un ierobežot sejas atpazīšanas tehnoloģiju izmantošanu. Eiropas Padome ir mudinājusi izstrādāt un pieņemt speciālu regulējumu attiecībā uz sejas atpazīšanas tehnoloģiju biometrisko apstrādi, ko veic

1 Feldstein, S. (2019). The Global Expansion of AI surveillance. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

2 Ravani, S. (17 July, 2019). Oakland bans use of facial recognition technology, citing bias concerns. *San Francisco Chronicle.* https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php; Lyons, K. (13 February, 2021). Minneapolis prohibits use of facial recognition software by its police department. *The Verge.* https://www.theverge.com/2021/2/13/22281523/minneapolis-prohibits-facial-recognition-software-police-privacy

valsts iestādes tiesībaizsardzības nolūkos, kā arī aizliegt konkrētus to izmantošanas veidus.[3] Eiropas Savienība izstrādā mākslīgā intelekta regulējumu, kurā īpaša uzmanība ir pievērsta biometrisko datu izmantošanai attālinātai identifikācijai tiesībaizsardzības nolūkos. Eiropas Komisijas 2020. gadā publicētajā Baltajā grāmatā par mākslīgo intelektu ir uzsvērts, ka biometrisko datu izmantošana un vākšana attālinātās identifikācijas nolūkos rada specifiskus riskus cilvēka cieņai, tiesībām uz privāto dzīvi un personas datu aizsardzību, kā arī citām pamattiesībām.[4]

2021. gada 21. aprīlī Eiropas Komisija nāca klajā ar jaunu Mākslīgā intelekta regulas priekšlikumu (MI akta priekšlikums).[5] Tas ir pasaulē pirmais priekšlikums, kas paredz mākslīgā intelekta jomas tiesisko regulējumu. MI akta priekšlikums nosaka konkrētu mākslīgā intelektā balstītas prakses veidu aizliegumu. Līdzās citiem aizliegumiem, piemēram, sociālajai novērtēšanai, kaitīgai manipulēšanai un personas uzvedības ietekmēšanai, ir paredzēts aizliegt arī reāllaika biometrisko attālinātās identifikācijas sistēmu izmantošanu sabiedriskās vietās tiesībaizsardzības nolūkos. Tomēr šo aizliegumu piemērošana ir ierobežota, kā arī ir paredzēti daudzi izņēmumi. MI akta priekšlikumā ietvertos noteikumus ir kritizējuši Eiropas Datu aizsardzības uzraudzītājs un Eiropas Datu aizsardzības kolēģija, aicinot aizliegt mākslīgā intelekta izmantošanu, lai automātiski atpazītu cilvēka pazīmes sabiedriskās vietās.[6]

Sejas atpazīšanas tehnoloģijas ir nonākušas arī Eiropas datu aizsardzības iestāžu redzeslokā. Francijas un Zviedrijas datu aizsardzības iestādes ir atzinušas, ka to izmantošana skolās pārkāpj Eiropas datu aizsardzības regulējumu.[7]

3 Council of Europe. (2021). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). Guidelines on Facial Recognition. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

4 Eiropas Komisija. (2020). Baltā grāmata par mākslīgo intelektu. Eiropiska pieeja – izcilība un uzticēšanās. https://op.europa.eu/lv/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

5 Eiropas Komisija. (2021). Priekšlikums. Eiropas Parlamenta un Padomes Regula, kas nosaka saskaņotas normas mākslīgā intelekta jomā (Mākslīgā intelekta akts) un groza dažus Savienības leģislatīvos aktus. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

6 EDPB, EDPS. (2021). EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https:// https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en

7 EDPB. (22 August, 2019). Facial recognition in school renders Sweden's first GDPR fine. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-zfirst-gdpr-fine_en; CNIL. (29 Octobre, 2019). Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.

Zviedrijas datu aizsardzības iestāde arī ir konstatējusi, ka Zviedrijas policija, izmantodama "Clearview AI" personu identificēšanai, ir pārkāpusi datu aizsardzības noteikumus.[8]

Pret sejas atpazīšanas tehnoloģiju izmantošanu sabiedriskās vietās arvien skaļāk iebilst nevalstiskās organizācijas. 2020. gada novembrī Eiropas Digitālo tiesību asociācija (EDRi) – Eiropas nevalstisko organizāciju tīkls, kas aizstāv pamattiesības digitālajā vidē, – uzsāka kampaņu "Atgūsti savu seju" (*Reclaim Your face* – angļu val.). 2021. gada februārī asociācija ierosināja Eiropas Pilsoņu iniciatīvu, aicinot Eiropas Komisiju stingri reglamentēt biometrisko tehnoloģiju izmantošanu un aizliegt šo tehnoloģiju, it īpaši sejas atpazīšanas tehnoloģiju, izmantošanu sabiedriskās vietās, jo tās var izraisīt nelikumīgu masveida novērošanu un ir pretrunā cilvēktiesībām.[9]

Ne tikai sejas atpazīšanas tehnoloģijas ir raisījušas lielas bažas par to ietekmi uz cilvēktiesībām un tiesiskumu. Satraukumu ir radījušas arī citas mākslīgā intelekta novērošanas tehnoloģijas, kas tiek izmantotas, ne tikai lai atpazītu sejas, bet arī lai novērotu emocijas un uzvedību, un to izmantošana profilēšanai un prognozēšanai.[10] Pēdējos gados visā pasaulē strauji pieaug tendence izmantot biometriskās tehnoloģijas. Biometriskās un emocionālās atpazīšanas tehnoloģijas arvien vairāk izmanto tiesībaizsardzības iestādes Eiropas valstīs, turklāt nenodrošinot pārredzamību, uzraudzību un sabiedrības līdzdalību. Biometriskās novērošanas tehnoloģijas, piemēram, sejas atpazīšana un algoritmiskās profilēšanas un prognozēšanas rīki, tiek testēti uz Eiropas robežām. Plašu kritiku izraisīja ES finansētais projekts "iBorderCtrl", kurā tika plānots testēt melu noteikšanas sistēmu imigrācijas kontrolei.[11] Sejas atpazīšanas tehnoloģijas tiesībaizsardzības iestādes un policija izmanto arī prognozēšanai, kas var balstīties uz iedzīvotāju uzvedības analīzi un vērtēšanu, lai apkarotu noziedzību. ES Mākslīgā intelekta augsta līmeņa ekspertu grupa (AI HLEG) ir uzsvērusi, ka

8 EDPB. (21 February, 2021). Swedish DPA: Police unlawfully used facial recognition app. https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_lv

9 EDRi. (17 February, 2021). New ECI calls Europeans to stand together for a future free from harmful biometric mass surveillance. https://edri.org/our-work/new-eci-ban-biometric-mass-surveillance/

10 Sk., piemēram, Mcstay, A. (2020). Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy, *Big Data & Society*, 7(1). https://doi.org/10.1177/2053951720904386

11 Stolton, S. (8 February, 2021). Commission under pressure in EU court over 'lie detector tech'. *EURACTIV* https://www.euractiv.com/section/digital/news/aommission-under-pressure-over-lie-detector-tech-in-eu-courts/. Sk. arī Gallagher, R., Jona, L. (26 July, 2019). We tested Europe's new lie detector for travelers – and immediately triggered a false positive. *The Intercept*. https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/

fizisku personu identificēšana, izmantojot biometriskos datus, piemēram, melu atpazīšana un personības vērtēšana, izmantojot mikroizteiksmes, un automātiskā balss atpazīšana, rada būtiskus tiesiskus un ētiskus izaicinājumus.[12] Lielu satraukumu ir radījusi arī policijas un tiesībaizsardzības iestāžu prakse arvien vairāk paļauties uz mākslīgā intelekta datu analīzes un prognozēšanas rīkiem, lai novērstu un kontrolētu noziedzību.[13]

Jau ilgstoši pastāv plašas diskusijas par robežām, cik tālu valsts var izmantot datu vākšanas un analīzes metodes un tehnoloģijas, lai veiktu novērošanu, lai aizsargātu tādas sabiedrības intereses kā valsts un sabiedrības drošība. Arvien pieaugošie drošības draudi ir veicinājuši masveida novērošanas praksi visā pasaulē. Edvarda Snoudena (*Edward Snowden*) atklājumi par ASV īstenoto slepeno masveida novērošanas programmu, kas tika ieviesta pēc 11. septembra teroraktiem un paredzēja plašu gan ASV pilsoņu, gan citu valstu, to skaitā Eiropas, iedzīvotāju telekomunikācijas un datu plūsmas novērošanu un pārtveršanu iepriekš neiedomājamos apmēros, aizsāka plašu globālu diskusiju par izlūkdienestu un tiesībaizsardzības iestāžu masveida novērošanas praksi, tās radīto būtisko aizskārumu cilvēktiesībām, īpaši tiesībām uz privātumu un datu aizsardzību, atbilstoša regulējuma trūkumu, kā arī efektīvu aizsardzības garantiju neesamību.[14]

Ne tikai ASV, bet arī Eiropā ir ieviesta plaša masveida novērošanas prakse, piemērojot dažāda veida pasākumus drošības nolūkos. Eiropas Savienības Tiesai (EST) un Eiropas Cilvēktiesību tiesai (ECT) līdz šim ir bijusi izšķiroša nozīme masveida novērošanas ierobežošanā un uzraudzībā, veicinot tiesību uz privātumu, datu aizsardzību un citu cilvēktiesību ievērošanu un aizsardzību.[15]

ES līmenī arī ir ieviesti daudzi masveida novērošanas pasākumi drošības interešu vārdā. Kā steidzams pretterorisma pasākums, reaģējot uz teroristu uzbrukumiem 2004. gadā Madridē un 2005. gadā Londonā, 2006. gadā ātri tika pieņemta

12 AI HLEG. (2019). Ethics Guidelines for Trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

13 Sk. McDaniel, J. L. M., Pease, K. G. (2021). Introduction. In: McDaniel, J. L. M., Pease, K. G. (eds.), *Predictive Policing and Artificial Intelligence*. Routledge, pp. 1–38; van Brakel, R. E. (2021). Rethinking predictive policing: Towards a holistic framework of democratic algorithmic surveillance. In: Schuilenburg, M., Peeters, R. (eds.), *Algorithmic Societies: Power, Knowledge and Technology in the Age of Algorithms*. Routledge, pp. 104–118.

14 Sk., piemēram, OHCHR. (2014). The right to privacy in the digital age. https://digitallibrary.un.org/record/777869

15 Sk. Nesterova, I. (2019). Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards. In: Ulrich, G., Ziemele, I. (eds.), *How International Law Works in Times of Crisis*. Oxford University Press, pp. 109–125.

ES Datu saglabāšanas direktīva[16], neņemot vērā iebildumus par tās neatbilstību pamattiesībām. 2014. gadā EST pieņēma spriedumu apvienotajās lietās "Digital Rights Ireland" un "Seitlinger u. c.", ar kuru pasludināja minēto direktīvu par spēkā neesošu, atzīstot, ka ar to uzliktais pienākums valstīm paredzēt, ka elektronisko pakalpojumu sniedzējiem ir jāsaglabā noteiktu kategoriju dati, rada nepamatotu iejaukšanos pamattiesībās.[17]

EST ir pieņēmusi vairākus spriedumus, kuriem par pamatu ir ASV masveida novērošanas prakse. Tā 2015. gadā pieņēma spriedumu "Schrems I" lietā[18] un 2020. gadā – "Schrems II" lietā[19], ar kuriem divas reizes atzina par spēkā neesošiem Eiropas Komisijas lēmumus par aizsardzības līmeņa pietiekamību datu nodošanai no ES uz ASV. Arī ECT ilgstoši turpina izskatīt daudzas lietas par valstu masveida novērošanas pasākumu atbilstību cilvēktiesībām, mēģinot noteikt robežas, cik tālu ir ierobežojamas personas tiesības uz privātumu, atsaucoties uz valsts un nacionālās drošības interesēm.[20] Plašā tiesu prakse apliecina, ka atcelt masveida novērošanas pasākumus, kas drošības nolūkos tiek ieviesti gan ES, gan nacionālā līmenī, ir ļoti grūti, un bieži vien tas ir iespējams tikai pēc ilgstošiem tiesvedības procesiem.

Līdzīgi kā terorisma un drošības draudi vēl lielākus jaunu novērošanas tehnoloģiju "plūdus" izraisīja Covid-19 krīze. Lai cīnītos ar pandēmijas izplatību, valstis visā pasaulē strauji ieviesa digitālās novērošanas tehnoloģijas, sākot no veselības lietotnēm, valkājamām aprocēm, kontaktu izsekošanas un citām mobilām lietotnēm un beidzot ar droniem un sejas atpazīšanas tehnoloģijām.[21] Šie eksperimenti ir būtiski satricinājuši cilvēktiesības, radot jaunus jautājumus, cik tālu var ierobežot privātumu, datu aizsardzību un citas cilvēktiesības, lai garantētu sabiedrības veselību un drošību, un kā līdzsvarot indivīda un sabiedrības intereses. Ārkārtas apstākļi neatceļ cilvēktiesību ievērošanas prasību.

16 Eiropas Parlamenta un Padomes Direktīva 2006/24/EK (2006. gada 15. marts) par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK. *OV L* 105, 13.04.2006. (spēkā līdz 03.05.2006.).

17 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C293/12 *Digital Rights Ireland* un C594/12 *Seitlinger* u. c., ECLI:EU:C:2014:238.

18 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems* pret *Data Protection Commissioner,* ECLI:EU:C:2015:650.

19 EST 2020. gada 16. jūlija spriedums lietā C-311/18 *Data Protection Commissioner pret Facebook Ireland Limited* un *Maximillian Schrems,* ECLI:EU:C:2020:559.

20 Sk. European Court of Human Rights. (2020). Guide on Article 8 of the Convention – Right to respect for private and family life https://www.echr.coe.int/documents/guide_art_8_eng.pdf

21 Couch, D. L., Robinson, P., and Komesaroff, P. A. (2020). COVID-19 – Extending Surveillance and the Panopticon. *Journal of Bioethical Inquiry*, 17, pp. 809–814. https://doi.org/10.1007/s11673-020-10036-5

Ir ārkārtīgi svarīgi steidzami risināt tiesiskos, ētiskos un sociālos jautājumus, kas saistīti ar mākslīgā intelekta un citu novērošanas tehnoloģiju izmantošanu. Tās var radīt jauna veida apdraudējumu cilvēktiesībām, ievērojami veicināt sabiedrības kontroli, balstoties uz tādiem mērķiem un vērtībām, kas var būt pretrunā ar demokrātiskas sabiedrības vērtībām. Ķīnas sociālā vērtēšanas un tā saucamā "sociālā kredīta" sistēma ir šīs tendences spilgtākais piemērs.[22]

Mākslīgā intelekta novērošanas tehnoloģijas atšķiras no iepriekšējām digitālās novērošanas formām. Mākslīgais intelekts piedāvā jaunas iespējas datu vākšanai, apstrādei un analīzei, ļauj veikt novērošanu daudz plašāk, detalizētāk un precīzāk, tādējādi ievērojami veicinot novērošanas pasākumu izmantošanu. Šīs tehnoloģijas rada jauna veida specifiskus apdraudējumus. Tās būtiski apdraud tiesības uz privātumu un datu aizsardzību, cilvēka cieņu un diskriminācijas aizlieguma principu, vārda un pulcēšanās brīvību un citas cilvēktiesības un brīvības, kā arī rada plašāku ietekmi uz sabiedrību, tiesiskumu un demokrātiju kopumā.[23] Mākslīgais intelekts ievērojami palielina gan valsts, gan lielo tehnoloģiju uzņēmumu masveida novērošanas apmērus un saasina varas nevienlīdzību. Grāmatas "Uzraudzības kapitālisma laikmets. Cīņa par cilvēka nākotni jaunajās varas robežās" autore Šošana Zubofa (*Shoshana Zuboff*) vērš uzmanību, ka novērošanas kapitālisms izraisa katastrofālas sekas demokrātijai un brīvībai, jo rada vēl nebijušu zināšanu un varas koncentrāciju, ko neregulē likumi un noteikumi. Šī zināšanu un varas asimetrija izraisa jaunas sociālās nevienlīdzības formas, ļauj ietekmēt indivīdu un iedzīvotāju uzvedību, kas ir antidemokrātiski.[24] Lai gan šī grāmata pamatā ir veltīta valsts masveida novērošanai un komerciālā novērošana ir ārpus tās pētāmo jautājumu loka, tajā pašā laikā izaicinājumi, ko rada komerciālā novērošana, it īpaši sociālo mediju platformu algoritmi, kas ietekmē un manipulē ar lietotāju viedokli un sociālo un politisko uzvedību, ir ne mazāk būtiski, un tiem būtu veltāms atsevišķs pētījums.

Lai nodrošinātu, ka mākslīgā intelekta novērošanas tehnoloģiju izmantošana atbilst cilvēktiesībām un tās neapdraud, ir ļoti svarīgi steidzami izvērtēt esošo

22 Kobie, N. (7 June, 2019). The Complicated truth about China's social credit system. *WIRED.* https://www.wired.co.uk/article/china-social-credit-system-explained

23 Sk. Council of Europe, CAHAI Secretariat. (2020). Towards regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law. https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a

24 Sk. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. *The Fight for a Human Future at the new Frontier of Power.* Profile Books, pp. 512–519. Sk. arī Naughton, J. (20 January, 2019). 'The goal is to automate us': welcome to the age of surveillance capitalism. *The Guardian.* https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

regulējumu, kā arī izstrādāt jaunu regulējumu, kas noteiktu skaidras robežas, kādos gadījumos mākslīgā intelekta tehnoloģijas var izmantot un kādos nevar, un kas paredzētu efektīvas aizsardzības garantijas un uzraudzības mehānismus. Steidzami ir jānosaka ierobežojumi mākslīgā intelekta novērošanas pasākumiem, lai garantētu līdzsvaru starp valsts un sabiedrības drošību, no vienas puses, un nepieciešamību aizsargāt cilvēktiesības un demokrātiju, no otras puses. Regulējums ir būtisks instruments, lai nodrošinātu atbildīgu un uz cilvēkiem vērstu mākslīgā intelekta izmantošanu un novērstu tā radīto apdraudējumu.

Pēdējo gadu laikā starptautiskās organizācijas, it īpaši Eiropas Padome[25], Apvienoto Nāciju Izglītības, zinātnes un kultūras organizācija (UNESCO)[26], Ekonomiskās sadarbības un attīstības organizācija (OECD)[27], ES[28], daudzas profesionālās organizācijas[29], nevalstiskās un citas organizācijas, kā arī tehnoloģiju uzņēmumi[30] strauji izstrādājuši un turpina izstrādāt mākslīgā intelekta ētikas vadlīnijas, lai definētu vērtības, principus un ietvaru ētiskai mākslīgā intelekta attīstībai. Tomēr arvien skaidrāk tiek uzsvērts, ka regulējumam ir jāiet tālāk par ētikas normām un gan starptautiskā, gan nacionālā līmenī ir jānosaka tiesiski saistošas prasības un jāievieš efektīvi praktiski mehānismi, kas nodrošinātu šo ētikas principu ieviešanu praksē. Gan starptautiskās organizācijas, gan valstis visā pasaulē šobrīd aktīvi meklē labāko veidu, kā tiesiski regulēt mākslīgo intelektu.

Tajā pašā laikā spēkā esošais tiesiskais regulējums, it sevišķi cilvēktiesību un datu aizsardzības regulējums, jau šobrīd ir piemērojams attiecībā uz mākslīgo intelektu. Cilvēka cieņa, tiesības uz privātumu un datu aizsardzību, diskriminācijas aizlieguma princips, vārda un pulcēšanās brīvība, kā arī citas cilvēka tiesības un brīvības ir īpaši nozīmīgas un piemērojamas attiecībā uz mākslīgā intelekta

25 Council of Europe. (2020). Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

26 UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137

27 OECD. (2019). Recommendation of the Council on Artificial Intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

28 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

29 Sk., piemēram, IEEE. (2019). Ethically Aligned Design. First Edition: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf?utm_medium=undefined&utm_source=undefined&utm_campaign=undefined&utm_content=undefined&utm_term=undefined

30 Sk. Fjeld, J., Achten, N., Hilligoss, H., et al. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Berkman Klein Center Research Publication No. 2020-1. https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y

novērošanas tehnoloģijām un var palīdzēt noteikt to izmantošanas tā sauktās sarkanās līnijas. Būtiskas prasības mākslīgā intelekta sistēmu izstrādei, ieviešanai un izmantošanai nosaka arī datu aizsardzības regulējums, it īpaši Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)[31] un Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīva (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu kriminālsodus, un par šādu datu brīvu apriti[32] (Policijas direktīva; *Law Enforcement Directive* – angļu val.), kura paredz datu vākšanas un izmantošanas noteikumus un stingras atbildības prasības.

Grāmatā tiek izvirzīta tēze, ka cilvēktiesību un datu aizsardzības standarti ir visdrošākais pamats mākslīgā intelekta regulējuma turpmākai attīstībai un ir nepieciešams izstrādāt skaidru tiesisko regulējumu, kas tālāk attīstītu starptautiskās cilvēktiesību normas un Eiropas datu aizsardzības regulējumu un noteiktu skaidrus mākslīgā intelekta novērošanas tehnoloģiju izmantošanas ierobežojumus. Tāpēc ir jāizvērtē esošā tiesiskā regulējuma atbilstība, efektivitāte un trūkumi un pēc tam jāapsver jauna regulējuma nepieciešamība. Jauns tiesiskais regulējums būtu jāpieņem tikai tad, kad jautājums ir pienācīgi izprasts, ir notikušas sabiedriskās diskusijas un ir konstatēts, ka spēkā esošie likumi nav pietiekami, lai risinātu noteiktus jautājumus.

Grāmatas mērķis ir izpētīt mākslīgā intelekta novērošanas tehnoloģiju ietekmi uz cilvēktiesībām, tām piemērojamo spēkā esošo regulējumu un tā turpmāko attīstību nākotnē, lai novērstu šo tehnoloģiju radītos riskus un apdraudējumu.

Monogrāfija ir pirmais zinātniskais pētījums Latvijas tiesību zinātnē, kurā analizēta un pētīta mākslīgā intelekta ietekme uz cilvēktiesībām un tiesiskais regulējums, kā arī novērošanas tehnoloģiju radītie riski un apdraudējums. Tā sniedz ieteikumus turpmākai regulējuma un politikas attīstībai starptautiskā un nacionālā līmenī.

31 Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (Dokuments attiecas uz EEZ). *OV L* 119, 04.05.2016.

32 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu kriminālsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI. *OV L* 119, 04.05.2016.

Grāmatā ir aplūkota mākslīgā intelekta novērošanas tehnoloģiju izmantošana tiesībaizsardzības jomā un to attīstības tendences gan Eiropā, gan citviet pasaulē un izvērtēts šo tehnoloģiju radītais apdraudējums cilvēktiesībām, kā arī ietekme uz sabiedrību un demokrātiju kopumā. Autore apskata, kā attīstās mākslīgā intelekta regulējums, lai ierobežotu novērošanas tehnoloģiju radītos riskus, un kā esošais cilvēktiesību un datu aizsardzības regulējums jau šobrīd regulē šīs tehnoloģijas. Tajā ir analizēts, kā tiesības uz privātumu un datu aizsardzību un to ierobežošanas nosacījumi, kas attīstīti ECT un EST praksē, ir piemērojami attiecībā uz mākslīgā intelekta novērošanas pasākumiem. Grāmata sniedz rekomendācijas, kā attīstīt mākslīgā intelekta novērošanas tehnoloģiju tiesisko regulējumu un kādas aizsardzības garantijas un mehānismi jāievieš praksē, lai nodrošinātu atbildīgu un uz cilvēku vērstu šo tehnoloģiju izmantošanu un novērstu to radīto apdraudējumu.

Grāmatā ir plaši analizēti Latvijas, starptautiskie un ārvalstu tiesību akti, instrumenti, politikas dokumenti un tiesu prakse, kā arī citi prakses materiāli. Būtiska nozīme monogrāfijā ir cilvēktiesību, datu aizsardzības, kā arī mākslīgā intelekta jomā tādu pieņemto tiesību aktu, vadlīniju un cita veida dokumentu analīzei, ko ir pieņēmušas vai šobrīd izstrādā ES, Eiropas Padome, ANO, UNESCO un OECD. Darbā ir izmantoti Eiropas valsts iestāžu, datu aizsardzības iestāžu un citu valsts institūciju, nevalstisko organizāciju izstrādātie dokumenti (piemēram, EDRi[33]), pētniecības institūtu (piemēram, Berkmana Kleina centra[34], *AI Now* institūta[35], Alana Tjūringa institūta[36]), Eiropas Savienības Pamattiesību aģentūras (FRA)[37] pētījumi. Tāpat darbā ir izmantoti dokumenti, ko izstrādājušas starptautiskās mākslīgā intelekta ekspertu grupas: Eiropas Padomes Mākslīgā intelekta *ad hoc* komiteja (CAHAI)[38], ES AI HLEG[39] un UNESCO Starptautiskā *ad hoc* ekspertu

33 EDRi. (12 January, 2021). Re: Open letter: Civil society call for the introduction of red lines in the upcoming European Commission proposal on Artificial Intelligence. https://edri.org/wp-content/uploads/2021/01/EDRi-open-letter-AI-red-lines.pdf

34 Fjeld, et al. (2020), Principled Artificial Intelligence.

35 Crawford, K., Roel, D., Theodora, D., et al. (2019). AI Now 2019 Report. New York, AI Now Institute. https://ainowinstitute.org/publication/ai-now-2019-report-2

36 Leslie D. (2020). Understanding bias in facial recognition technologies: an explainer. The Alan Turing Institute. https://doi.org/10.5281/zenodo.4050457

37 FRA. (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement. https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

38 Council of Europe, CAHAI. (2020). Feasibility Study. https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

39 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

grupa Rekomendācijas par mākslīgā intelekta ētiku izstrādei (AHEG)[40]. Grāmatā ir arī plaši analizēta un salīdzināta ECT un EST judikatūra. Lai gan galvenokārt ir analizēti mākslīgā intelekta tiesiskie aspekti, darbā plaši izmantota starpdisciplinārā pieeja. Lai izprastu mākslīgā intelekta novērošanas sistēmas un atklātu ne tikai to tiesisko, bet arī sociālo un ētisko ietekmi, kā arī ietekmi uz sabiedrību un demokrātiju, līdzās pētījumiem tiesību zinātnē ir izmantots plašs klāsts pētījumu (grāmatu, zinātnisko rakstu, ziņojumu un citu dokumentu) socioloģijā, ētikā, filozofijā, politikā, tehnoloģijā un citās jomās.

Grāmatas mērķauditorija ir plaša. Tā būs noderīgs materiāls tiesību zinātņu un citu sociālo un humanitāro zinātņu, kā arī tehnoloģiju, dabaszinātņu un medicīnas zinātņu pētniekiem un akadēmiskajiem mācībspēkiem, kā arī studentiem. Pētījuma rezultāti un politikas ieteikumi būs vērtīgs informācijas avots likumdevējam, kā arī tiesām un citām valsts, tiesībaizsardzības un uzraudzības institūcijām, lai izstrādātu regulējumu un politiku, ieviestu uzraudzības pasākumus un atbildības mehānismus uzticamam mākslīgajam intelektam un veicinātu tiesisku, ētisku, atbildīgu un uz cilvēku vērstu mākslīgā intelekta attīstību. Pētījums var būt noderīgs iestādēm un uzņēmumiem, kas izstrādā, ievieš un izmanto mākslīgā intelekta un citas jaunās tehnoloģijas, un nevalstiskajām organizācijām, lai veicinātu sabiedrības iesaisti un informētu par mākslīgā intelekta un citu jauno tehnoloģiju ietekmi uz cilvēktiesībām, to radītajiem riskiem un apdraudējumu. Visbeidzot, grāmata ir paredzēta ikvienam lasītājam, kurš vēlas uzzināt vairāk par mākslīgā intelekta regulējuma attīstību, tā ietekmi uz cilvēktiesībām un datu aizsardzības tiesībām.

Temats tiek apskatīts septiņās nodaļās. Darba pirmā nodaļa iepazīstina ar tematu un skaidro, kas ir mākslīgais intelekts un valsts novērošana no sociālā un tehnoloģiskā skatpunkta, atklājot, kā jauno tehnoloģiju attīstība no lielajiem datiem līdz mākslīgajam intelektam ir ietekmējusi un veicinājusi masveida novērošanu. Vispirms tiek izskaidrots, ko nozīmē mākslīgais intelekts, kā tas ir saistīts ar lielajiem datiem, personas datiem un profilēšanas jēdzienu. Pēc tam tiek skaidrots novērošanas jēdziens, varas nevienlīdzība kā novērošanas pazīme, kā arī masveida novērošanas nošķiršana no mērķtiecīgas novērošanas, un apskatīts, kā jau ilgstoši valsts un sabiedrības drošība ir bijusi par pamatu dažādu masveida novērošanas pasākumu ieviešanai. Tālāk nodaļa atklāj, kādā veidā mākslīgais intelekts ir ievērojami palielinājis novērošanas praksi, un aplūko mākslīgā intelekta tehnoloģijas un metodes – sejas atpazīšanas tehnoloģijas, emociju uztveršanas tehnoloģijas (*emotion recognition technologies* – angļu val.), kā arī prognozēšanu

40 UNESCO, AHEG. (2020). Outcome document: First Draft of the Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000373434

tiesībaizsardzības nolūkos (*predictive policing* – angļu val.), kā arī atklāj, kā Covid-19 krīze ir veicinājusi digitālo novērošanas tehnoloģiju izmantošanu.

Darba otrā nodaļa apskata mākslīgā intelekta novērošanas pasākumu ietekmi uz cilvēktiesībām. Atsevišķi tiek apskatītas cilvēktiesības, kuras visvairāk ietekmē minētie pasākumi: cilvēka cieņa; tiesības uz privātumu un datu aizsardzību; diskriminācijas aizlieguma princips; bērnu tiesības; tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu; izteiksmes brīvība; pulcēšanās un biedrošanās brīvība. Grāmata apskata, kā minētās tiesības ir regulētas starptautiskajos un Eiropas cilvēktiesību dokumentos, it īpaši Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijā (ECTK)[41] un Eiropas Savienības Pamattiesību hartā (Harta)[42], kā arī Latvijas Republikas Satversmē[43], un izvērtē, kā šīs tiesības apdraud masveida novērošanas pasākumi, vienlaikus atklājot arī šo tehnoloģiju plašāku ietekmi uz sabiedrību, tiesiskumu un demokrātiskām vērtībām. Nodaļas beigās ir apskatīts pienākums ievērot cilvēktiesības krīzes situācijā, uzsverot, ka arī tādās ārkārtas situācijās, kādu radīja, piemēram, Covid-19, iedzīvotājiem nav jāizvēlas starp cilvēktiesību ievērošanu un tādu interešu aizsardzību kā sabiedrības drošība un veselība.

Grāmatas trešā nodaļa aplūko privātuma nozīmi, ko īpaši būtiski aizskar masveida novērošanas pasākumi. Lai attaisnotu aizskarošu tehnoloģiju un prettiesisku datu izmantošanu, ir bijuši daudzi mēģinājumi mazināt privātuma nozīmi, un šīm tiesībām ir veltīta plaša kritika. Nodaļā tiek atklāts, kādu labumu un aizsardzību sniedz privātums, kāpēc tas ir jāaizsargā. Apskatītas dažādas teorijas un analizēts, kāds ir tiesību uz privātumu pamatojums un nozīme, lai ierobežotu mākslīgā intelekta masveida novērošanas pasākumus. Nodaļā aplūkota tiesību uz privātumu attīstība un ka tās ietver: tiesības palikt vienam; tiesības kontrolēt informāciju par sevi; cilvēka cieņas, autonomijas un rīcības brīvības būtisku aspektu; aizsardzību pret varas ļaunprātīgu izmantošanu. Nodaļā ir aplūkota šo tiesību aizsardzība starptautiskos cilvēktiesību dokumentos un atklāts, kā tās palīdz aizsargāt arī citas cilvēktiesības, piemēram, izteiksmes un pulcēšanās brīvību. Tāpat tiek atklāts, kā privātums arvien vairāk tiek skatīts kā sabiedrības kopīga vērtība, kas kā cilvēka cieņas neatņemams elements un ētikas pamatvērtība jauno tehnoloģiju laikmetā aizsargā pret visaptverošu novērošanu un varas asimetriju, kā arī uzsvērta privātuma apzināšanās nozīme. Nodaļas nobeigumā vērsta uzmanība, ka Covid-19 pandēmijas radītā krīze ievērojami satricinājusi

41 Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija. Pieņemta 04.11.1950. (EP, Latvijā spēkā no 27.06.1997.). *Latvijas Vēstnesis*, 13.06.1997., Nr. 144/145.

42 Eiropas Savienības Pamattiesību harta. Pieņemta 07.12.2000. *OV C* 2020/239, 07.06.2016.

43 Latvijas Republikas Satversme. Pieņemta 15.02.1922. (spēkā no 07.11.1922.). *Latvijas Vēstnesis*, 01.07.1993., Nr. 43.

tiesības uz privātumu un ir steidzami nepieciešams pieņemt atbilstošus politikas pasākumus, to skaitā regulējumu, lai nepieļautu, ka masveida novērošana kļūst par jauno normu.

Grāmatas ceturtajā nodaļā ir aplūkota datu aizsardzības tiesību attīstība un mākslīgā intelekta regulējuma aizsākumi. Sākumā ir sniegts īss ieskats, kā datu aizsardzības tiesības iezīmē informācijas un komunikācijas tehnoloģiju regulējuma aizsākumu, mēģinot samērot dažāda vieda valsts un privātā sektora intereses. Nodaļas turpinājumā ir aplūkots, kā starptautiskās organizācijas – Eiropas Padome, OECD, ANO, UNESCO – ir attīstījušas datu aizsardzības tiesības, un sniegts vispārīgs pārskats, kā minētās organizācijas ir iesaistījušās diskusijā par masveida novērošanas apdraudējumu cilvēktiesībām, kā arī izvērtēts, kā šīs organizācijas ir sākušas darbu pie mākslīgā intelekta regulējuma izstrādes. Pēc tam nodaļā ir aplūkota ES datu aizsardzības regulējuma attīstība. Vispirms ir atklāts, kā pakāpeniski pieaugusi cilvēktiesību nozīme ES un kā tiesības uz datu aizsardzību Hartā atšķirībā no ECTK un citiem starptautiskajiem cilvēktiesību līgumiem tika noteiktas kā atsevišķas pamattiesības. Tiek uzsvērts, ka ES uz pamattiesībām balstītajai pieejai, kas ir pamatā datu aizsardzības regulējuma attīstībai, vajadzētu būt arī mākslīgā intelekta tehnoloģiju regulējuma turpmākās attīstības pamatā. Pēc tam ir aplūkota ES datu aizsardzības reforma un Vispārīgā datu aizsardzības regula (VDAR), kā arī speciālais datu aizsardzības regulējums, īpaši Policijas direktīva. Nodaļas beigās ir aplūkota mākslīgā regulējuma attīstība ES. Nodaļā ir atklāts, ka gan starptautiskā, gan ES līmenī arvien vairāk tiek pieprasīts skaidrs tiesiskais regulējums, kas noteiktu ierobežojumus, aizsardzības garantijas un prasības, kā arī sarkanās līnijas mākslīgā intelekta tehnoloģiju izmantošanai.

Piektā nodaļa analizē tiesību uz privātumu un datu aizsardzību ierobežošanu EST un ECT masveida novērošanas lietās. Vispirms ir īsi izskaidroti ECTK un Hartā noteiktie datu aizsardzību ierobežošanas nosacījumi. Tālāk nodaļā ir aplūkotas būtiskākās ECT lietas, kurās izvērtēta valsts novērošanas pasākumu atbilstība cilvēktiesībām, kā arī EST prakse novērošanas lietās, kas saistītas ar ES tiesību aktu spēkā esamību vai interpretāciju. Pēc tam ir detalizēti analizētas četras būtiskākās aizsardzības garantijas, kas identificētas aplūkotajās pārnacionālo tiesu lietās: skaidrs, precīzs un pieejams regulējums; samērīgums un nepieciešamība; neatkarīgs uzraudzības mehānisms; efektīvi tiesiskās aizsardzības līdzekļi. Nodaļā ir uzsvērts, ka ECT un EST praksē būtiskākais nosacījums, lai varētu veikt masveida novērošanas pasākumus, ir pienākums izvērtēt, vai šādi pasākumi ir "stingri" jeb "absolūti" nepieciešami konkrētā mērķa sasniegšanai un vai tie ir samērīgi jeb proporcionāli ar noteikto mērķi, kas ir piemērojams arī mākslīgā intelekta novērošanas pasākumiem.

Grāmatas sestā nodaļa analizē datu aizsardzības pamatprasības mākslīgā intelekta novērošanas tehnoloģijām. Aplūkoti un salīdzināti noteikumi, kas

ietverti dažādos tiesību aktos: VDAR, kas paredz vispārējās prasības, Policijas direktīvā, kas ir piemērojama attiecībā uz tiesībaizsardzības iestādēm, kā arī Konvencijā 108+. Nodaļā vispirms ir skaidrots, kas ir personas dati un biometriskie dati, aplūkoti dažādi sejas atpazīšanas tehnoloģiju izmantošanas veidi. Pēc tam analizēti personas datu apstrādes principi , kas ir pamatā un jāpiemēro, interpretējot visas pārējās datu aizsardzības prasības, – likumīgumu, nolūka ierobežojuma principu, datu minimizēšanu, precizitāti, glabāšanas ierobežojumu, datu drošību un atbildības principu. Nodaļā ir analizēta automatizēta lēmumu pieņemšana un cilvēka līdzdalības prasība, datu subjekta tiesības, kas ir piemērojamas arī attiecībā uz masveida novērošanas tehnoloģijām. Pēc tam ir aplūkota viena no visbūtiskākajām atbildības prasībām – novērtējums par ietekmi uz datu aizsardzību. Autore atklāj galvenos problēmjautājumus un regulējuma nepilnības, kas rada izaicinājumus datu aizsardzības prasību piemērošanai attiecībā uz mākslīgā intelekta novērošanas tehnoloģijām, īpašu uzmanību veltot sejas atpazīšanas tehnoloģijām. Nodaļas nobeigumā ir atsevišķi aplūkoti datu aizsardzības standarti, kas ietverti starptautisko organizāciju izdotajās rekomendācijās kontaktu izsekošanas lietotnēm, kādus izaicinājumus tie ir radījuši praksē, un vērsta uzmanība uz nepieciešamību šos standartus piemērot arī attiecībā uz mākslīgā intelekta novērošanas tehnoloģijām.

Darba pēdējā – septītā – nodaļa apkopo galvenos secinājumus un sniedz vairākus ieteikumus, kā attīstīt tālāk mākslīgā intelekta tiesisko regulējumu, kas balstās uz cilvēktiesībām un nosaka sarkanās līnijas, un kādi pārvaldības mehānismi un aizsardzības garantijas ir jāievieš praksē, lai nodrošinātu atbildīgu, uzticamu mākslīgā intelekta tehnoloģiju izmantošanu un lai aizsargātu un novērstu apdraudējumu cilvēktiesībām, demokrātijai un tiesiskumam.

1. DAĻA

Mākslīgais intelekts un valsts novērošana

Lai varētu izprast mākslīgā intelekta novērošanas tehnoloģijas un to ietekmi uz cilvēktiesībām, vispirms nodaļā ir skaidroti daži tehniskie aspekti – ko nozīmē jēdziens "mākslīgais intelekts", kā tas ir saistīts ar lielajiem datiem un personas datiem. Pēc tam aplūkots, kā mākslīgais intelekts ir ietekmējis masveida novērošanas pasākumu attīstību, kurus valsts tiesībaizsardzības iestādes ievieš drošības nolūkos. Tālāk ir aplūkotas mākslīgā intelekta novērošanas tehnoloģijas, kas šobrīd ļoti strauji attīstās – sejas atpazīšanas tehnoloģijas, emociju uztveršanas tehnoloģijas, prognozēšana tiesībaizsardzības nolūkos, kā arī dažādi digitālie novērošanas pasākumi, ko valstis ieviesa, lai cīnītos ar Covid-19 pandēmiju.

1.1. Mākslīgā intelekta, lielo datu un novērošanas izpratne

1.1.1. Mākslīgā intelekta jēdziens un izpratne

Nepastāv viena universāla mākslīgā intelekta definīcija, bet gan daudzas definīcijas, kas cenšas skaidrot mākslīgā intelekta jēdzienu. Turklāt tās attīstās līdz ar tehnoloģiju progresu.

Viena no pazīstamākajām, kā arī plašākajām mākslīgā intelekta definīcijām to skaidro kā centienus automatizēt intelektuālos uzdevumus, ko parasti veic cilvēki. Mākslīgā intelekta sistēmas darbojas ar zināmu autonomiju, lai sasniegtu iepriekš noteiktu mērķi, un šīs darbības parasti ir uzdevumi, kuriem citādi būtu nepieciešama cilvēka intelektuālo spēju izmantošana.[44]

Termins "mākslīgais intelekts" ietver nepārprotamu atsauci uz intelekta jēdzienu. Tomēr šī definīcija nav saistīta ar cilvēka intelekta aizstāšanu, bet gan ar rezultātu, ko sasniedz sistēma. Šo pieeju vislabāk izskaidro slavenais Tjūringa tests, ko Alans Tjūrings (*Alan Turing*) izvirzīja 1950. gadā. Tas apgalvo, ka mašīnu var uzskatīt par "inteliģentu", ja cilvēks, kas ar to mijiedarbojas, nevar pateikt, vai darītājs ir persona vai dators.[45] Tomēr mākslīgā intelekta sistēmas intelekts nebūt nav līdzīgs cilvēka intelektam.

Gan saistībā ar mašīnām, gan cilvēkiem "intelekts" ir neskaidrs jēdziens, kaut arī to ir ilgi pētījuši psihologi, biologi un neirozinātnieki. Tāpēc mākslīgā

44 Sk. Fjeld, et al. (2020). Principled Artificial Intelligence.

45 Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind,* 49, pp. 433–460. https://www.csee.umbc.edu/courses/471/papers/turing.pdf

intelekta pētnieki galvenokārt izmanto racionalitātes jēdzienu. Tas attiecas uz spēju izvēlēties pareizāko rīcību, lai sasniegtu noteiktu mērķi, ņemot vērā noteiktus optimizējamus kritērijus un pieejamos resursus.[46] Stjuarts Rasels (*Stuart Russell*) un Pīters Norvigs (*Peter Norvig*) definē mākslīgo intelektu kā tādu "inteliģentu aģentu" projektēšanu un veidošanu, kuri spēj uztvert apkārtējo vidi un veikt darbības, kas ietekmē šo vidi.[47] Mākslīgais intelekts vienkāršoti tiek definēts kā sistēmu spēja izmantot algoritmus, mācīties no datiem un pieņemt lēmumus līdzīgi, kā to darītu cilvēki.[48]

Eiropas Komisija mākslīgo intelektu ir ieteikusi uzskatīt par sistēmu, kas spēj demonstrēt inteliģentu rīcību, analizējot apkārtējo vidi, un ar zināmu autonomiju veikt darbības, lai sasniegtu konkrētus mērķus.[49] Šī Eiropas Komisijas definīcija ir izmantota Eiropas Parlamenta priekšlikumā Regulai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrādes, ieviešanas un izmantošanas ētikas principiem, kurā mākslīgais intelekts ir definēts kā "sistēma, kura darbojas, pamatojoties uz programmatūru, vai ir iestrādāta tehnikas ierīcēs un kuras rīcība liecina par intelektu, *inter alia* vācot, apstrādājot, analizējot un interpretējot datus par tā apkārtējo vidi un ar zināmu autonomijas pakāpi veicot darbības, ar kurām tā sasniedz konkrētus mērķus" (4. panta a) punkts).[50]

Viena no precīzākajām mākslīgā intelekta definīcijām ir sniegta Ētikas vadlīnijās uzticamam mākslīgajam intelektam, kuras 2019. gadā izstrādāja AI HLEG: "Mākslīgā intelekta (MI) sistēmas ir programmatūras (un, iespējams, arī aparatūras) sistēmas, kuras izstrādājis cilvēks un kuras, pastāvot sarežģītam mērķim, darbojas fiziski vai digitāli, uztverot apkārtējo vidi kā ievadītus datus, interpretējot savāktos strukturētos vai nestrukturētos datus, izdarot spriedumus par zināšanām vai apstrādājot no šiem datiem iegūto informāciju, kā arī pieņemot lēmumus par labāko rīcību konkrētā mērķa sasniegšanai. Mākslīgā intelekta sistēmas var izmantot simboliskus noteikumus vai mācīties

46 AI HLEG. (2019). A definition of Artificial Intelligence: main capabilities and scientific disciplines. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

47 Russel, S. J., Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*. Pearson Series in Artificial Intelligence. Hoboken: Pearson.

48 Rouhiainen, L. (2019). *Artificial Intelligence: 101 Things You Must Know Today about Our Future*, CreateSpace Independent Publishing Platform, p. 3.

49 Eiropas Komisija. (2018). Komisijas paziņojums. Mākslīgais intelekts Eiropai. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52018DC0237&from=EN

50 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru (2020/2012(INL)). https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_LV.html#title2

no cipariska modeļa, kā arī pielāgot savu darbību, analizējot, kā to iepriekšējā rīcība ir ietekmējusi vidi."[51]

Lielākā daļa mākslīgā intelekta sistēmu veic tikai daļu no definīcijā uzskaitītajām darbībām: modeļu atpazīšanu (piemēram, augu vai dzīvnieku attēlu, cilvēku sejas vai izteiksmes atpazīšana), valodu apstrādi (piemēram, runas valodu izpratne, tulkošana no vienas valodas uz citu, cīņa pret surogātpastu vai atbildēšana uz jautājumiem), praktisku ieteikumu sniegšanu (piemēram, pirkumu ieteikšana, informācijas atlase, rūpniecisko procesu optimizēšana) utt. Tajā pašā laikā dažas sistēmas var apvienot daudzas šādas spējas, piemēram, pašvadāmie transportlīdzekļi vai militārie un aprūpes roboti.[52] Mākslīgā intelekta sistēmas var būt gan tīri programmatiskas, piemēram, virtuālie asistenti, attēlu analīzes sistēmas, meklētājprogrammas, runas un sejas atpazīšanas sistēmas, gan arī aparatūrā ietvertas sistēmas, piemēram, robotos, pašbraucošās automašīnās, dronos un lietu internetā.

AI HLEG mākslīgo intelektu kā zinātnes disciplīnu apraksta šādi: "Mākslīgais intelekts kā zinātnes disciplīna ietver dažādas pieejas un paņēmienus, piemēram, mašīnu mācīšanos (konkrēti piemēri – mašīnu dziļā mācīšanās un stimulētā mācīšanās), mašīnu spriešanu (ietver plānošanu, programmu veidošanu, zināšanu reprezentāciju un spriešanu, meklēšanu un optimizēšanu) un robotiku (ietver kontroli, uztveri, sensorus un iedarbinātājus, kā arī pārējo paņēmienu integrēšanu kiberfiziskās sistēmās)."[53]

Mākslīgais intelekts ir vispārīga joma, kas ietver mašīnmācīšanos un dziļo mācīšanos, taču tajā ietilpst arī daudz citu darbību, kas neiekļauj mācīšanos. Piemēram, agrīnās šaha programmas izmanto tikai stingri kodētus noteikumus.

Patlaban mākslīgā intelekta galvenie virzieni ir: problēmu risināšana (piemēram, plānošana un meklēšana), zināšanu un pamatojuma izstrāde (attiecas uz lēmumu pieņemšanu), mašīnmācīšanās (ietver dziļo mācīšanos, neironu tīklus), mijiedarbība (piemēram, robotika, cilvēka aģenta un robota mijiedarbība), dabiskās valodas apstrāde (tulkošana, informācijas iegūšana), uztveres attīstīšana (redzes spējas un attēla atpazīšana).[54]

Mašīnmācīšanās ir viens no primārajiem mākslīgā intelekta virzieniem. Tā ir datu analīzes metode, kas izmanto mācību algoritmus, lai automatizēti atklātu

51 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

52 Sk. Sartor, G., Lagioia, F. (2020). The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence. European Parliament. http://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

53 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

54 François, C., Allaire, J. J. (2018). *Deep Learning with R*. Shelter Island, NY: Manning Publications Co, p. 4. Sk. Dignum, V. (2019). *Responsible Artificial Intelligence. How to Develop and Use AI in a Responsible Way*. Springer, p. 12.

modeļus lielās datu kopās, ģenerētu modeļus un izmantotu tos prognozēm. Mašīnmācīšanās sistēmas tiek apmācītas, nevis tieši programmētas.[55] Tām ir iespēja mācīties no tā, kā tiek izmantotas, lai tās spētu piedāvāt personalizētu lietotāja pieredzi. Viens no zināmākajiem piemēriem ir personalizēšana, ko varam redzēt, piemēram, "Meta" ("Facebook") un citās sociālo mediju platformās un "Google" meklētājprogrammas rezultātos.

Viens no straujāk augošajiem mākslīgā intelekta novirzieniem ir dziļā mācīšanās, kas ir mašīnmācīšanās apakšnozare. Dziļā mācīšanās izmanto vairāku slāņu neironu tīklus, lai atpazītu sarežģītas attiecības un modeļus datos. Dziļās mācīšanās algoritmi var atpazīt un kategorizēt informāciju un identificēt modeļus. Tas ļauj mākslīgā intelekta sistēmām nepārtraukti mācīties darbībā un uzlabot rezultātu kvalitāti un precizitāti, nosakot, vai lēmumi ir pareizi.[56]

Mākslīgie neironu tīkli, kurus bieži dēvē vienkārši par neironu tīkliem, savu nosaukumu ir guvuši, iedvesmojoties no bioloģiskajiem neironu tīkliem, lai gan tie darbojas ļoti atšķirīgi. Neironu tīklam ir ievade – dati, kas nāk no sensoriem, un izvade – attēla interpretācija. Tīkla apmācības posmā, analizējot piemērus, savienojumu svarīgums tiek pielāgots, lai pēc iespējas vairāk atbilstu pieejamiem piemēriem, tas ir, lai samazinātu kļūdu starp paredzamo un tīkla aprēķināto izvadi. Apmācības posma beigās notiek neironu tīkla rīcības testēšanas fāze, kurā, izmantojot iepriekš neredzētus piemērus, tiek pārbaudīts, vai uzdevums ir labi iemācīts.[57] Ir svarīgi ņemt vērā, ka šai pieejai, tāpat kā visām mašīnmācīšanās metodēm, vienmēr ir noteikts kļūdas procents, lai arī tas parasti ir mazs. Tāpēc svarīgs faktors ir precizitāte, pareizo atbilžu procentuālā attiecība.

Mākslīgā intelekta sistēmas tiek apmācītas, balstoties uz ārējās pasaules datiem vai arī cilvēka veidotās vides apmācāmajiem datiem, tādējādi pieņemtie lēmumi un to kvalitāte kļūst tieši atkarīga no šo datu avota, kvalitātes un objektivitātes. Dziļo mašīnmācīšanās metožu algoritmiskie rezultāti ir grūti interpretējami, kā rezultātā šo mākslīgā intelekta sistēmu pieņemtie lēmumi var nebūt izskaidrojami. Proti, neviens nevar pateikt, kādēļ lēmumi ir tieši tādi un ne citādi.[58]

55 François, C., Allaire, J. J. (2018). *Deep Learning with R*. Shelter Island, NY: Manning Publications Co, p. 4. Sk. Dignum, V. (2019). *Responsible Artificial Intelligence. How to Develop and Use AI in a Responsible Way*. Springer, p. 5.

56 Sk. François, Allaire (2018), *Deep Learning with R*, pp. 8–11; Dignum (2019), *Responsible Artificial Intelligence*, pp. 27–28.

57 AI HLEG. (2019). A definition of Artificial Intelligence.

58 Sk. Barredo Arrieta, Díaz-Rodríguez, N., Del Ser, J. et al. (2020). Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI. *Information Fusion,* 58, pp. 82–115. https://doi.org/10.1016/j.inffus.2019.12.012; VARAM. (2020). Informatīvais ziņojums "Par mākslīgā intelekta risinājumu attīstību". https://www.varam.gov.lv/lv/jauns-informativais-zinojums-par-maksliga-intelekta-risinajumu-attistibu

Ir jānošķir šobrīd esošās mākslīgā intelekta iespējas no nākotnes iespējām. Visattīstītākā mākslīgā intelekta sistēma vēl joprojām ir t. s. šaurais mākslīgais intelekts, kas izstrādāts, lai risinātu konkrētus uzdevumus vai problēmas. Šaurais mākslīgais intelekts tiek pretstatīts vispārīgam mākslīgam intelektam. Ja tiktu izstrādāts vispārīgs mākslīgais intelekts, autonomās mašīnas kļūtu spējīgas uz vispārīgu saprātīgu darbību un varētu veikt plašu uzdevumu klāstu. Tāpat kā cilvēki tas būtu spējīgs vispārināti un abstrakti mācīties, izmantojot dažādas kognitīvās funkcijas, tam būtu asociatīvā atmiņa, un tas spētu spriest un pieņemt lēmumus.[59] Pašreiz mēs varam runāt par vispārīgo mākslīgo intelektu tikai kā par hipotētisku attīstības iespēju tālākā nākotnē. Lai gan tādu mākslīgo intelektu varam redzēt vienīgi zinātniskās fantastikas filmās un grāmatās un mums nav jābaidās no robotiem, kas pārņems pasauli, tajā pašā laikā mākslīgais intelekts pēdējo gadu laikā attīstās zibens ātrumā un jau šobrīd rada ne tikai daudz ieguvumu dažādās jomās, piemēram, izglītības, veselības, vides, transporta jomā, bet var arī radīt būtiskus apdraudējumus sabiedrībai, kurus ir nepieciešams novērst.

Kaut arī mākslīgais intelekts kā zinātnes disciplīna ir pastāvējis jau kopš 20. gadsimta 50. gadiem, tikai nesen tas kļuvis par vispārzināmu jēdzienu. Var rasties jautājums, kāpēc mākslīgais intelekts tieši pēdējos gados ir kļuvis tik populārs. Tā straujo attīstību ir ietekmējuši trīs būtiski aspekti. Pirmkārt, pēdējo gadu laikā ir izdevies savākt agrāk nepieredzētu milzīgu datu daudzumu. Otrkārt, tiek izstrādāti arvien efektīvāki algoritmi. Treškārt, ir kļuvusi pieejama ļoti liela skaitļošanas jauda. Šo trīs elementu apvienojums ir ļāvis mākslīgajam intelektam ļoti strauji attīstīties. Vienkāršoti, mākslīgo intelektu var dēvēt par tehnoloģiju kopumu, kas apvieno datus, algoritmus un datošanas jaudu.[60] Mākslīgā intelekta sadalīšana šajos trīs pamatelementos ļauj labāk uztvert saistību starp mākslīgo intelektu un citiem jēdzieniem, kas iepriekš jau izraisījuši politikas izmaiņas un diskusijas šajā jomā. Viens no tādiem ir lielie dati.

1.1.2. Mākslīgais intelekts un lielie dati

Pašlaik viena no galvenajām politiskajām prioritātēm ir mākslīgais intelekts un tā regulējuma izstrāde, bet agrāk plašas diskusijas un daudzi regulējuma priekšlikumi bija saistīti ar lielajiem datiem un to radītajiem izaicinājumiem, it īpaši datu aizsardzībai.

Lielie dati būtiski maina veidu, kādā informācija tiek vākta, apvienota un analizēta. Lielie dati, kas galvenokārt balstās uz mijiedarbību ar citu tehnoloģisko vidi, piemēram, lietu internetu un mākoņdatošanu, var sniegt nozīmīgu labumu

59 OECD. (2017). OECD Digital Economy Outlook 2017. https://doi.org/10.1787/9789264276284-en

60 Eiropas Komisija (2020), Baltā grāmata par mākslīgo intelektu.

un inovācijas sabiedrībai, uzlabojot biznesa produktivitāti, valsts sektora darbību, kā arī sabiedrības līdzdalību. Lielie dati var sniegt vērtīgu informāciju, kas ļauj saprast un pārvaldīt sabiedrību.

Pastāv daudzas lielo datu definīcijas, kas atšķiras atkarībā no konkrētās disciplīnas. Lielākā daļa no tām koncentrējas uz pieaugošo tehnoloģisko spēju savākt, apstrādāt un iegūt jaunas un paredzamas zināšanas no liela apjoma datiem, to ieguves ātruma un daudzveidības. Termins "lielie dati" parasti apzīmē ārkārtīgi lielas datu kopas, kuras var aprēķināt skaitliski, lai iegūtu secinājumus par datu modeļiem, tendencēm un korelācijām. Kā norāda Starptautiskā telekomunikāciju savienība, lielie dati ir "paradigma, kas ļauj apkopot, uzglabāt, pārvaldīt, analizēt un vizualizēt, iespējams, ar reāllaika ierobežojumiem, plašu datu kopu ar neviendabīgām īpašībām".[61]

Definīcija "lielie dati" ietver lielo datu analīzi.[62] Galvenie jautājumi, kas saistīti ar datu aizsardzību, attiecas ne tikai uz apstrādāto datu apjomu, ātrumu un daudzveidību, bet arī uz datu analīzi, izmantojot programmatūru, lai iegūtu jaunas un paredzamas zināšanas lēmumu pieņemšanai par personām un personu grupām.[63]

Mākslīgā intelekta sistēmu izstrāde, kas balstīta uz mašīnmācīšanos, veicina milzīgu datu kopu – lielo datu – izveidi. Lai mākslīgais intelekts varētu mācīties, tam ir nepieciešams milzīgs datu apjoms, ko analizēt, un tas pieprasa arvien vairāk datu.

Tajā pašā laikā digitalizācija ir notikusi pirms lielākās daļas mākslīgā intelekta sistēmu izveides. Datu plūsmas tiek veidotas visur, kur tiek izmantota skaitļošana. Mūsu digitālās pasaules pamatā ir nepārtraukta datu plūsma. Katru sekundi milzīgus datu apjomus iegūst un apstrādā daudz un dažāda veida sistēmas un ierīces, piemēram, sistēmas, kuras izmanto, lai veiktu ekonomiskos darījumus (piemēram, e-komercijā); sensori, kas uzrauga un nodrošina fizisko objektu darbību (piemēram, transportlīdzekļos vai viedo māju ierīcēs); darbplūsmas, ko rada ekonomiskas un valdības darbības (piemēram, banku, transporta vai nodokļu jomā);

61 ITU. (2015). Recommendation Y.3600. Big data – Cloud computing based requirements and capabilities. https://www.itu.int/rec/T-REC-Y.3600-201511-I/en

62 Terminu "lielo datu analīze" lieto, lai identificētu skaitļošanas tehnoloģijas, kas analizē lielu datu apjomu ar mērķi atklāt slēptos modeļus, tendences un korelācijas. Eiropas Savienības Kiberdrošības aģentūra skaidro, ka termins "lielo datu analītika" attiecas uz visu datu pārvaldības dzīves ciklu, kurā tiek vākti, organizēti un analizēti dati, lai atklātu modeļus, secinātu situācijas vai stāvokļus, prognozētu un izprastu uzvedību. Sk. arī ENISA. (2015). Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. https://www.enisa.europa.eu/publications/big-data-protection

63 Council of Europe. (2017). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (T-PD). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. https://rm.coe.int/16806ebe7a

novērošanas ierīces (piemēram, videokameras satiksmes kontrolei vai piekļuves kontroles sistēmas); sistēmas, ko izmanto nekomerciālām darbībām (piemēram, piekļuve internetam, meklēšana vai sociālie tīkli) utt.

Informācijas un datu apjoms pasaulē turpina pieaugt neiedomājami strauji. Pēdējo gadu laikā šīs datu plūsmas ir integrētas globālā savienotā datu apstrādes infrastruktūrā, kuras centrā ir internets. Šī infrastruktūra ir universāls līdzeklis saziņai, piekļuvei datiem un jebkura veida privātu un sabiedrisku pakalpojumu sniegšanai. Tā ļauj iedzīvotājiem iepirkties, izmantot banku un citus pakalpojumus, maksāt nodokļus, saņemt valsts pabalstus un tiesības, piekļūt informācijai un zināšanām, kā arī veidot sociālos kontaktus.

Digitālās pēdas atstāj gandrīz katra mūsu ikdienas darbība – ikviena dalīšanās ar ziņu vai "patīk" nospiešana, ziņas vai fotogrāfijas aplūkošana "Facebook", "Linkedin", "Twitter", "Instagram", katrs nosūtītais e-pasts vai ziņa koplietošanas platformās, meklēšana internetā, iepirkšanās "Amazon", mūzikas klausīšanās "Spotify", filmas skatīšanās "Netflix", skriešana vai pastaiga laukā, ja līdzi ir fitnesa aproce vai mobilais telefons, kurā ir instalētas lietotnes, kas vāc atrašanās vietas datus.

Datu apjoms, kas tiek radīts internetā pasaulē katru minūti, ir šokējoši liels. 2020. gadā ikvienu minūti "Google" tiek veikti vairāk nekā 4 miljoni meklējumu, "YouTube" skatīti 4,7 miljoni video, "WhatsApp" un "Facebook Masanger" nosūtīti 59 miljoni ziņu, kā arī nosūtīti 190 miljoni e-pasta vēstuļu. Turklāt ar katru gadu radīto datu apjoms strauji palielinās.[64]

Mobilo un interneta pakalpojumu un piekļuves ieviešana ir būtiski mainījusi datu vākšanas, analīzes un izmantošanas raksturu. 21. gadsimtā dati kļūs par lielāko vērtību, par ko sacenšas gan privātās kompānijas, gan valsts iestādes. Ikviens vēlas kontrolēt šo datu plūsmu, jo tā sniedz varu.

Lielie tehnoloģiju uzņēmumi, piemēram, "Google", "Meta" ("Facebook") un "Apple", sacenšas par to, lai piesaistītu mūsu uzmanību arvien vairāk, ne tikai lai varētu pārdot reklāmas, bet arī lai iegūtu arvien lielāku datu daudzumu. Šie interneta tehnoloģiju milži ir izveidojuši tā saukto uzmanības ekonomiku, kur galvenā prece ir cilvēka uzmanība. Digitālā joma ir veidota tā, lai cilvēki atdotu savu vērtīgo laika, uzmanības un datu resursus, neņemot vērā izmaksas, ko tas rada šīm personām un citiem.[65] Dati nav vērtība tikai tāpēc, ka tos var pārdot. Tehniski ne

64 Aystin, D. (16 April, 2021). Here is Your 2021 Internet Minute Infographic!: eDiscovery Trends. *eDiscoveryToday.* https://ediscoverytoday.com/2021/04/16/here-is-your-2021-internet-minute-infographic-ediscovery-trends/

65 Lewandowsky, S., Smillie, L., Garcia, D. et al. (2020). Technology and Democracy: Understanding the influence of online technologies on political behaviour and decision-making. Publications Office of the European Union, Luxembourg. https://data.europa.eu/doi/10.2760/709177

"Facebook", ne "Google" nepārdod datus, bet gan varu ietekmēt. Tie vāc, saglabā un analizē datus, lai varētu pārdot varu – varu parādīt reklāmas, varu piesaistīt uzmanību, varu ietekmēt uzvedību. "Google" un "Facebook" tikai tehniski nodarbojas ar datu biznesu, pamatā tas ir varas bizness. Personas dati pat vairāk nekā naudas pieaugums piešķir varu tiem, kas tos vāc un analizē, un tieši šī vara mūsu datus padara tik iekārojamus.[66]

Datu daudzums, ko mēs saražojam, turpinās palielināties, strauji pieaugot lietu internetam – visu veidu ierīcēm, sensoriem un mašīnām, kas ir savienotas un savstarpēji sazinās. Globālā savstarpēji saistītā datu apstrādes infrastruktūra ietver aptuveni 30 miljardus ierīču – datorus, viedtālruņus, mašīnas, kameras utt. –, kas ģenerē milzīgus datu apjomus.[67]

Ne visi dati, kas tiek apstrādāti lielo datu kontekstā, ir personas dati un saistīti ar mijiedarbību ar cilvēkiem, taču liela daļa attiecas uz tiem, tieši ietekmējot personas un viņu tiesības attiecībā uz personas datu apstrādi. Turklāt, tā kā lielie dati ļauj savākt un analizēt lielu datu apjomu, lai identificētu attieksmes modeļus un prognozētu grupu un kopienu uzvedību, ir jāņem vērā arī tas, ka ar datu izmantošanu saistītajiem riskiem ir kolektīva dimensija.[68]

Mākslīgā intelekta tehnoloģijas palielina datu apstrādes spējas veikt lielo datu analīzi un datu sasaisti un ir būtiski mainījušas datu vākšanas, analīzes un izmantošanas raksturu. Pateicoties mākslīgā intelekta metožu, milzīgā datu apjoma un skaitļošanas jaudas kombinācijai, ir kļuvis iespējams automātiski prognozēt un novērtējumus balstīt uz daudz vairāk piemēriem, ņemot vērā daudz lielāku skaitu katram no tiem piemītošu pazīmju jeb īpašību kopumu, lai panāktu daudz augstāku precizitātes līmeni. Tas tiek izmantots dažādiem mērķiem, piemēram, mērķorientētai reklāmai, kas balstīta uz ierakstiem par patērētāja īpašībām un uzvedību, piemēram, dzimumu, vecumu, pirkumu vēsturi.

Personas var pakļaut novērošanai un ietekmei dažādos veidos un kontekstos, balstoties uz plašu personisko īpašību kopumu, sākot no ekonomiskiem apstākļiem, veselības situācijas, dzīvesvietas, personiskās dzīves izvēlēm un notikumiem, uzvedības utt. Ar atbilstošām klasifikācijas un prognozēšanas metodēm analizējot un salīdzinot datus par personām, mākslīgais intelekts palielina profilēšanas iespējas, un tas ļauj izsecināt informāciju par šīm personām vai grupām un uz tā pamata veikt novērtējumu un pieņemt lēmumus.

66 Véliz, C. (2021). *Privacy Is Power: Why and How You Should Take Back Control of Your Data.* Bantam Press, p. 49.

67 Statista. (2019). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

68 Sk. Council of Europe (2017), Consultative Committee of the Convention for the Protection .. (T-PD).

Termins "profils" ir cēlies no itāļu valodas vārda *profilo*, kas nāk no *profilare* un sākotnēji nozīmē 'vilkt līnijas', it īpaši objekta kontūras. Tieši tā ir profilēšanas ideja, izmantojot datu apstrādi, respektīvi, paplašināt pieejamos datus par dažādu grupu indivīdiem, lai ieskicētu (aprakstītu vai paredzētu) viņu iezīmes un tieksmes.[69] Profilēšanas radītos draudus varēja spilgti redzēt "Cambridge Analytica" lietā, kas saistīta ar mēģinājumiem ietekmēt balsotāju rīcību ASV 2016. gada vēlēšanās, pamatojoties uz masveida personas datu apstrādi.[70]

Patlaban nostiprinās pastāvīga, uz datiem balstīta prognozēšanas pasaule, kurā mēs, iespējams, vairs nespēsim izskaidrot lēmumu iemeslus, un tas rada daudzus jaunus riskus un apdraudējumus. Arvien vairāk lēmumu cilvēku vietā pieņem algoritmi, kurus turklāt mēs nesaprotam. Lielo datu algoritmu novērošana attiecas uz visiem, jo tie fiksē un analizē katru darbību internetā. Mēs arvien vairāk paļaujamies uz lielo datu algoritmiem, piemēram, "Google" meklēšanas rezultātiem, "Google Map" maršrutiem, "Amazon" ieteikumiem, ko pirkt, "YouTube" ieteikumiem, ko klausīties, "Netflix" ieteikumiem, ko skatīties, utt. Platformas izmanto "ieteikumu" sistēmas, lai atlasītu to, kas katram ir visatbilstošākais – nākamais videoklips, ko mēs skatāmies, nākamais nopērkamais produkts, nākamais viedoklis vai jaunumi mūsu sociālo mediju ziņu plūsmas augšdaļā. Algoritmi nosaka, kādas grāmatas mums lasīt, kādas filmas skatīties, kādu mūziku klausīties, pa kādu maršrutu braukt, kur dzīvot, uz kurieni braukt atpūsties, kur mācīties, ar ko satikties utt. Ir grūti saprast, kā tie pieņem lēmumus un vai tie sniedz precīzu priekšstatu par pasauli. Arvien biežāk uzticamies algoritmiem, taču nesaprotam to pieņemtos lēmumus un arvien vairāk kļūstam kā marionetes šo algoritmu rokās. Šiem algoritmiem var būt arī nopietna ietekme uz mūsu autonomiju, nosakot to, kā redzam apkārtējo pasauli. Spēja pašiem pieņemt lēmumus ir būtisks cilvēka autonomijas aspekts, ko mēs pakāpeniski zaudējam. Arvien lielāka paļaušanās uz algoritmiem rada neapturamu tendenci, ka cilvēki arvien vairāk tiek pakļauti lēmumiem, ko pieņēmušas mākslīgā intelekta sistēmas vai kas pieņemti ar to palīdzību. Turklāt šie lēmumi var būt grūti saprotami un apstrīdami, un dažkārt tie var ļoti būtiski ietekmēt cilvēka dzīvi.

Mākslīgā intelekta sistēmas tiek izmantotas, ne tikai lai ietekmētu lietotāju un patērētāju rīcību un izvēles, bet tās arvien vairāk lieto gan privātie uzņēmumi, gan valsts iestādes, lai pieņemtu lēmumus, kas skar personas un kam var būt būtiska ietekme. Arvien vairāk algoritmisko lēmumu pieņemšanas sistēmas tiek izmantotas lēmumu pieņemšanas atbalstam. Daudzās situācijās šādu lēmumu ietekme var būt ļoti nozīmīga, piemēram, ja tas ir saistīts ar izglītību, nodarbinātību,

69 Sk. Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

70 Sk. EDPS. (2018). Opinion 3/2018. EDPS Opinion on online manipulation and personal data. https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

veselības aizsardzību, kredīta piešķiršanu, soda noteikšanu un tiesas spriedumiem. Algoritmu prognozes var tikt izmantotas, lai pieņemtu dažāda veida lēmumus, piemēram, klienta kredītspējas noteikšanai, darba pieteikumu izvērtēšanai un pat lai noteiktu, kādu atzīmi skolēns saņems vidusskolas gala eksāmenā.[71] Tiesībaizsardzības iestādes var izmantot tos, lai prognozētu, vai persona izdarīs noziedzīgu nodarījumu un uz tā pamata būtu arestējama, kaut gan šīs prognozes var būt kļūdainas un diskriminējošas.

Liela daļa problēmu ir saistītas ar inteliģento mašīnu spēju vai, precīzāk, spējas trūkumu pieņemt ētiskus lēmumus un lēmumu pieņemšanas procesā ņemt vērā cilvēciskās vērtības un ētiskos principus. Viens no lielākajiem izaicinājumiem ir, kā nodrošināt, ka algoritmisko lēmumu pieņemšanas sistēmas būtu taisnīgas. Tās var būt diskriminējošas dažāda veida aizspriedumu dēļ, kas izriet no apmācības datiem, tehniskiem ierobežojumiem vai arī sabiedrības vai individuāliem aizspriedumiem. Vairākumā gadījumu rezultāts būs netaisnīgs un diskriminējošs tad, ja tas nesamērīgi ietekmē noteiktas grupas bez pieņemama pamatojuma. Šādas sistēmas var radīt un veicināt aizspriedumus pret noteiktas grupas locekļiem, ja uz šo grupu attiecas tikai ļoti maza daļa no apmācāmajiem datiem, jo tas samazina paredzamības precizitāti attiecībā uz šo grupu. Piemēram, sejas atpazīšanas algoritmi, kas tiek izstrādāti, pamatā izmantojot baltādainu vīriešu fotoattēlus, būs daudz mazāk precīzi un to piemērošana būs diskriminējoša pret sievietēm un citas etniskās piederības cilvēkiem.

Viena no mākslīgā intelekta attīstības tendencēm, kas šobrīd ļoti strauji attīstās un var radīt būtisku apdraudējumu cilvēktiesībām, ir masveida novērošanas tehnoloģijas, it īpaši sejas atpazīšanas un citas biometriskās tehnoloģijas. Tomēr, pirms analizējam konkrētas mākslīgā intelekta tehnoloģijas un to radītos riskus, īsumā apskatīsim, ko nozīmē novērošana un kā tā ir attīstījusies līdz mūsdienu datu un mākslīgā intelekta laikmetam.

1.1.3. Digitālās masveida novērošanas attīstība

1.1.3.1. Novērošanas jēdziens

Novērošanas jēdzienam pašam par sevi ir gara vēsture tiesiskuma, tiesībaizsardzības un izlūkošanas zinātniskajās un filozofiskajās diskusijās. Kaut arī novērošanas (*surveillance* – angļu val.) definīcijas atšķiras, lielākā daļa zinātnieku uzsver, ka tā ir kas vairāk nekā tikai skatīšanās, tā ir atkarīga arī no spējas kontrolēt,

71 Mayer-Schonberger, V., Cukier, K. (2017). *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight*. London: John Murray, p. 17.

regulēt vai ietekmēt uzvedību.[72] Vārds "novērošana" ir cēlies no franču valodas vārda *surveillance*, kas nozīmē 'skatīties pāri' jeb 'skatīties no augšas'.[73] Etimoloģiski tas izriet no latiņu valodas vārda *vigilare*, kas nozīmē 'uzraudzīt', 'apsargāt', 'skatīties'.[74] Tas nenozīmē tikai pasīvu skatīšanos vai novērošanu, bet gan pārraudzību, kas veikta ar mērķi pieņemt kādus lēmumus un iejaukties, lai mainītu uzvedību.

Termina "novērošana" vietā var arī lietot vārdu "uzraudzība"[75], kas arī atspoguļo šo darbību mērķi "kontrolēt" vai "regulēt" sabiedrību. Ar terminu "uzraudzība" tiesībaizsardzības kontekstā tiek saprasta cilvēku vai grupu novērošana, kas veikta, izmantojot personas datu sistēmas, lai regulētu vai vadītu viņu uzvedību.[76] Turklāt, lai tā būtu efektīva, nav nepieciešams, lai cilvēki zinātu par šādas uzraudzības veikšanu, gluži pretēji – slepenai uzraudzībai pat ir lielāks spēks. Tajā pašā laikā vārds "uzraudzība" tiek lietots ļoti dažādos kontekstos, piemēram, uzraudzības mehānismi un uzraudzības iestādes. Sabiedrībā plašāk lietots ir termins "novērošana", piemēram, visiem zināmas ir videonovērošanas tehnoloģijas. Tāpēc grāmatā pamatā tiek lietots jēdziens "novērošana", bet atkarībā no konteksta dažkārt darbā var tikt izmantots arī otrs jēdziens.

Var izšķirt dažādus novērošanas veidus. 1971. gadā Alans Vestins (*Alan Westin*) darbā "Informācijas tehnoloģijas demokrātijā" identificēja trīs novērošanas formas, ko var izmantot valsts iestāde: fiziskā, psiholoģiskā un datu. Fiziskā novērošana ietver personas fizisku novērošanu vai noklausīšanos, psiholoģiskā – ietver nopratināšanas formas, kā arī personības testus, ko izmanto darba devēji, savukārt datu novērošana ietver informācijas atklāšanu, kas notiek, veicot ikvienu darbību, tās vākšanu un saglabāšanu.[77] Tomēr par datu novērošanu nevar uzskatīt ikvienu datu apstrādes procesu.

Datu novērošana ir attiecināma uz datu apstrādi un izmantošanu sistēmās, kas galvenokārt saistītas ar novērošanas veikšanu, bet ne uz tādu apstrādi, kurai

72 Monahan, T., Wood, D. M. (2018). Introduction. Surveillance Studies as a Transdisciplinary Endeavor. In: Monahan, T., Wood, D. M. (eds.), *Surveillance Studies: A Reader*. New York: Oxford University Press.

73 Ibid.

74 Moore, P. V. (2020). *Data subjects, digital surveillance, AI and the future of work*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf

75 No angļu valodas vārdu "*surveillance*" var tulkot gan kā 'uzraudzība', gan 'novērošana'.

76 Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the ACM* 31(5), 498–512. Sk. Ferguson, A. G. (2017). Big data Surveillance: The Convergence of Big data and Law Enfocement, p. 171. In: Gray, D., Henderson, S. E. (eds), *The Cambridge Handbook on Surveillance Law.* Cambridge University Press, pp. 171–197.

77 Lloyd, I. J. (2020). *Information Technology Law*. 9th ed. Oxford: Oxford University Press, pp. 11–12.

ir citi mērķi.[78] Vienlaikus jāpatur prātā, ka sākotnējie sistēmas izmantošanas mērķi var tikt mainīti un arī jau pieejamie dati vēlāk var tikt izmantoti novērošanas sistēmās, piemēram, fotogrāfiju datubāzes var izmantot sejas atpazīšanas sistēmu izstrādē.

Līdz ar tehnoloģiju, datu vākšanas, glabāšanas un analīzes metožu attīstību datu novērošana ir kļuvusi par galveno un izplatītāko novērošanas veidu, ko izmanto gan valsts un tiesībaizsardzības iestādes, gan privātie uzņēmumi dažādu savu interešu vārdā. To var dēvēt arī par digitālo vai elektronisko novērošanu, kas ietver dažādus veidus: audio, vizuālo, metadatu, komunikācijas, biometrisko novērošanu jeb uzraudzību. Turklāt robežas starp dažādām novērošanas formām izzūd, piemēram, fiziskā novērošana var notikt, izmantojot lokalizācijas datus, kā arī videonovērošanas kameras.

Sākotnēji novērošanu veica valsts tiesībaizsardzības iestādes, savukārt tagad to arvien plašāk izmanto privātie uzņēmumi. Dati un tehnoloģijas ir būtiskais faktors, kas veicinājis valsts iestāžu kontroli jeb varu pār iedzīvotājiem, kā arī lielo tehnoloģiju uzņēmumu kontroli pār lietotājiem.

1.1.3.2. Varas nevienlīdzība kā novērošanas pazīme

Veicot novērošanu, vienmēr pastāv varas nevienlīdzība. Privātā sektorā pastāv nevienlīdzīgas pozīcijas starp lielajiem tehnoloģiju un sociālo mediju uzņēmumiem un lietotājiem. Uzmanības resursi ir ierobežoti, bet pieprasījums pēc informācijas algoritmiskai apstrādei strauji aug. Tas ir radījis ļoti asimetriskas attiecības starp sociālo mediju platformām un to lietotājiem. Platformām ir dziļas zināšanas par lietotāja uzvedību un pat intīmiem dzīves aspektiem, savukārt lietotāji maz zina par to, kā tiek vākti viņu dati, kā tie tiek izmantoti komerciāliem vai politiskiem mērķiem un kā šie dati tiek izmantoti, lai veidotu lietotāju tiešsaistes pieredzi. Šī zināšanu asimetrija izpaužas arī kā varas asimetrija.

Zināt par citiem, vienlaikus maz atklājot par sevi, ir vissvarīgākais komerciālās varas veids uzmanības ekonomikā jeb ekonomikā, ko nosaka patērētāju uzmanība. Novērot citus, vienlaikus izvairoties, lai paši netiktu novēroti, ir arī galvenā autoritārās politiskās varas pazīme.[79] Š. Zubofa norāda, ka valsts īstenotas novērošanas apvienojums ar kapitālisma sistēmā veiktu novērošanu nozīmē, ka digitālās tehnoloģijas visu sabiedrību sadala divās grupās: vērotāji (neredzami,

78 Gstrein, O. J. (2020). Mapping Power and Jurisdiction on the Internet through the Lens of Government-Led Surveillance. *Internet Policy Review*, 9(3). https://doi.org/10.14763/2020.3.1497

79 Lewandowsky, Smillie, Garcia, et al. (2020), Technology and Democracy.

nezināmi un bez atbildības) un vērojamie. Zināšanu asimetrija nozīmē varas asimetriju, kam savukārt ir dziļas sekas uz demokrātiju.[80]

Varas nevienlīdzība izpaužas daudzās jomās. Nevienlīdzīgās pozīcijās atrodas darbinieki un darba devējs, kurš tos novēro, piemēram, izsekodams darbinieku datorus, izmantojot videonovērošanu vai pat emociju uztveršanas tehnoloģijas darbavietā. Nevienlīdzīgas attiecības pastāv arī starp iedzīvotājiem, kurus novēro, un valsti, kas veic dažādus novērošanas pasākumus tādu sabiedrībai nozīmīgu interešu vārdā kā drošība, un tie bieži vien ir slepeni, iedzīvotāji netiek par tiem informēti.

Valsts novērošana vienmēr ir bijusi atzīta par daļu no valsts suverenitātes īstenošanas. Novērošana ir viens no galvenajiem instrumentiem cīņā pret terorismu, un tai ir būtiska nozīme izlūkošanas pasākumu veikšanā, lai novērstu teroraktus un aizturētu teroristus. Bet, kā spilgti parādīja 2013. gada Edvarda Snoudena atklājumi, šīs darbības var arī būtiski ierobežot pamattiesības, it īpaši privātumu un datu aizsardzību.

Visai pasaulei ļoti liels pārsteigums bija ASV Nacionālās drošības aģentūras (NSA) bijušā darbinieka Edvarda Snoudena atklājumi par ASV īstenoto slepeno masveida elektroniskās novērošanas programmu, kas bija saistīta gan ar ASV pilsoņu, gan citu valstu personu telekomunikācijas un datu plūsmas novērošanu iepriekš neiedomājamos apmēros. 2013. gadā žurnālos "The Guardian"[81] un "The Washington Post" tika publicēti raksti, kas atklāja, ka ASV darbojas slepena masveida elektroniskās novērošanas programma, kura ļauj piekļūt ASV vadošo interneta uzņēmumu, tostarp "Microsoft", "Yahoo", "Google", "Facebook", "Skype", "YouTube", "Apple", interneta datiem, piemēram, e-pastiem, nosūtītajām ziņām, video, fotoattēliem, pārsūtītajiem failiem, darbībām sociālajos tīklos. Tika atklāts, ka NSA un ASV Federālais izmeklēšanas birojs pieslēdzās tieši šo interneta uzņēmumu serveriem, lai izsekotu tiešsaistes saziņu uzraudzības programmas ietvaros, kas zināma kā PRISM. Turklāt tie atklāja plašu datu apmaiņu starp tā saukto "Five Eyes" izlūkošanas tīklu, kurā ietilpst Lielbritānija, ASV, Austrālija, Kanāda un Jaunzēlande un kurā dominē NSA, kā arī plašu sadarbību starp

80 Zuboff (2019), *The Age of Surveillance Capitalism*, pp. 188–189, 281; Naughton (20 January, 2019), 'The goal is to automate us'.

81 Sk. Greenwald, G., MacAskill, E. (7 June, 2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian.* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; Ackerman, S., Rushe, D. (3 February, 2014). The Microsoft, Facebook, Google and Yahoo release US surveillance requests. *The Guardian*. http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests

dažādu ES dalībvalstu izlūkošanas iestādēm – it īpaši starp Lielbritānijas un Vācijas – un ASV iestādēm.[82]

Šie atklājumi iepriekš nebija zināmi ne tikai plašākai sabiedrībai, bet arī lielākajai daļai politisko lēmumu pieņēmēju un izraisīja globālu sašutumu. Vairāk nekā 1000 akadēmiskās sabiedrības pārstāvju parakstīja dokumentu, lai iebilstu pret masveida komunikāciju novērošanas praksi.[83] Arī starptautiskās organizācijas vērsa uzmanību uz šādas novērošanas prakses negatīvo ietekmi uz cilvēktiesībām. 2014. gadā ANO pieņēma ziņojumu, kurā nosoda nelikumīgu vai patvaļīgu komunikācijas uzraudzību un pārtveršanu, kā arī personas datu vākšanu, it īpaši, ja tā tiek veikta masveidā kā darbības, kas būtiski aizskar tiesības uz privātumu un vārda brīvību un var būt pretrunā ar demokrātiskas sabiedrības principiem.[84]

Līdz šim uzmanība pamatā ir pievērsta masveida novērošanai kā valsts un vēlāk arī privāto uzņēmumu piespiedu un pamatā slepenai varas īstenošanas formai. Tomēr līdz ar tās milzīgajiem apmēriem, kas turpina strauji augt, kā arī arvien plašāku akceptēšanu no sabiedrības puses, bet vienlaikus arī ar personu informētību mūsdienās tā ieņem citu formu un rada arī jaunus riskus personu tiesībām.

Modernās informācijas un komunikācijas tehnoloģijas tās atturošās ietekmes (*chilling effect* – angļu val.) dēļ var novest pie tā, ka indivīdi novēro un uzrauga cits citu un īsteno varu paši pār sevi bez jebkādas piespiešanas. Ne tikai tieša novērošana, bet arī apziņa, ka tevi var novērot, var likt personai mainīt savu uzvedību. Tas ir galvenais aspekts arī Džeremija Bentama (*Jeremy Bentham*) slavenajā *Panopticon* cietuma projektā, un tas arī bija attēlots Džordža Orvela (*George Orwell*) nozīmīgajā romānā "1984", kurā pilsoņi apzinājās, ka katru darbību var novērot policija, un tāpēc mēdza mainīt savu uzvedību.

Viens no ietekmīgākajiem uzraudzības pētniekiem ir Mišels Fuko (*Michel Foucault*), viņš veicināja pastiprinātu interesi par šo jomu. Fuko izmantoja Džeremija Bentama koncepciju par noteikta veida cietuma dizainu – panoptikonu –, kur sardzes tornis atrodas tieši apļveida cietuma centrā un kameras bez sienām ir vērstas uz iekšu. Uzraugi varēja vērot ieslodzītos, kuri nekad nezināja, vai viņi tiek novēroti. Ieslodzītie nevar zināt, vai kāds sēž centrālajā tornī un vai viņus vēro citi ieslodzītie no cietuma pagalma. Sociālā panoptikuma metafora ir tā,

82 Gellman, B., Poitras, L. (7 June, 2013). Washington Post: U.S., British intelligence mining data from nine US Internet companies in broad secret program. *Government Accountability Project.* https://whistleblower.org/in-the-news/washington-post-us-british-intelligence-mining-data-nine-us-internet-companies-broad/

83 Glaser, A. (12 February, 2014). Academics and Researchers Against Mass Surveillance. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2014/02/academics-and-researchers-against-mass-surveillance

84 OHCHR (2014), The right to privacy in the digital age.

ka novērošana neietver tikai zināmu vērotāju, kurš meklē, piemēram, aizdomās turēto, kurš pastāvīgi slēpjas, bet arī to, ka sabiedrība arvien vairāk tiek veidota tā, lai mudinātu mūs visus vērot citam citu.[85] Mūsdienu konteksts, ko raksturo arvien sarežģītāku novērošanas līdzekļu attīstība, vēl vairāk līdzinās Bentama "Panopticon" projektam nekā 19. un 20. gadsimta sabiedrība, kuru pētīja Fuko. Lielākā daļa novērošanas pētījumu akcentē Fuko panoptikona interpretācijas piespiedu vai represīvo pusi, kas uzsver varas būtisku pārsvaru. Tomēr viņš ir interpretējis to arī kā pašdisciplīnas praksi, kā to īpaši uzsver Bentams, tādējādi paplašinot "skatiena spēku", iekļaujot tajā visu veidu datu vākšanu un vizuālo novērošanu.[86]

No Bentama rakstiem par "panoptisko" vidi var secināt trīs galvenos elementus: "uzrauga" klātbūtne, ko nodrošina viņa pilnīga neredzamība; objektu universālā redzamība un pieņēmums, ka novērotie tiek novēroti pastāvīgi. Kaut arī varētu teikt, ka mums tagad ir daudz vairāk "novērotāju", ja ar redzamību mēs domājam iespēju piekļūt informācijai par personu – par viņa gaumi, interesēm, ienākumu līmeni, vecuma grupu, vēlamajām atpūtas aktivitātēm, vaļaspriekiem, politisko pārliecību, atrašanās vietu, iepirkšanās veidiem, interneta meklēšanas vēsturi, izmantotajām lietotnēm utt. Tas viss ir platformu kapitāla galvenais "izejmateriāls", kas tiek pastāvīgi vākts, apstrādāts un kas ir saistīts ar peļņu. Turklāt digitālās tehnoloģijas kā mūsdienu sabiedrības "panoptikas" iestatījumi nodrošina dažādus paškontroles un pašcenzūras veidus.[87]

Pašdisciplīnas un pašierobežošanas īstenošanai ir svarīgi, lai novērotie objekti saprastu, ka tie ir universāli un pastāvīgi redzami. Šāda apzināšanās ir notikusi, it īpaši pateicoties Edvardam Snoudenam, kurš atklāja NSA novērošanas apjomu, tostarp iegūstot datus no digitālajām platformām, piemēram, "Facebook", "Google", "Yahoo" utt., kā arī citiem prettiesiskiem "slēptiem" datu iegūšanas gadījumiem, piemēram, no politisko konsultāciju uzņēmuma "Cambridge Analytica" un "Facebook" skandāla. Šī apzināšanās rada "atturošu efektu" – lietotāju pašcenzūru – un īpaši ietekmē vārda brīvību. Jaunās tehnoloģijas arī mūsdienu sabiedrībā rada dažādus paškontroles un pašcenzūras veidus. Tādējādi mūsdienās būtiska atšķirība ir starp divām novērošanas formām – mērķtiecīgu konkrētu personu novērošanu un vispārīgāku jeb masveida novērošanu.

1.1.3.3. Mērķtiecīga un masveida novērošana

Tradicionālā jeb t. s. mērķtiecīga novērošana (*targeted surveillance* – angļu val.) ir nošķirama no masveida digitālās novērošanas (*mass surveillance* – angļu val.).

85 Moore, P. V. (2020). Data subjects, digital surveillance, AI and the future of work.

86 Manokha, I. (2018). Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance & Society*, 16(2), pp. 219–237. https://doi.org/10.24908/ss.v16i2.8346

87 Ibid.

Novērošana ir viena no galvenajām metodēm, ko izmanto tiesībaizsardzības iestādes, lai novērstu, izmeklētu un atklātu noziedzīgus nodarījumus.

Tradicionālā novērošanā tiek veikta aizdomās turēto personu vai iespējamo noziedzīgo darbību novērošana. Noziedzīgu nodarījumu atklāšanā sen jau tiek izmantoti personu attēli un videoieraksti. Videonovērošana, kas kļuva plaši pieejama 20. gadsimta 60. un 70. gados, ļāva tiesībaizsardzības iestādēm ātri identificēt personas un atklāt noziedzīgus nodarījumus.

Attīstoties tehnoloģijām, tiesībaizsardzības iestāžu darbība ir ļoti mainījusies. Ir izveidoti daudzi informācijas centri un sistēmas, kurās tiek vākti, apkopoti dati, kā arī notiek apmaiņa ar tiem, piemēram, no sodāmības reģistriem, biometriskajiem datiem, atrašanās vietas datiem, noziedzīgu nodarījumu novēršanas, izmeklēšanas un atklāšanas nolūkā. Tiek izmantotas tādas metodes kā slēpta sarunu noklausīšanās, telekomunikāciju un metadatu iegūšana.[88] Šāda novērošana tiek veikta visas sabiedrības interesēs, lai atklātu noziedzīgus nodarījumus un garantētu sabiedrisko drošību. Tā vienmēr sākas ar aizdomām pret konkrētu personu vai personām, un uz šo aizdomu pamata tiek veikta "mērķtiecīga" novērošana.

Mērķtiecīga novērošana var būt prettiesiska, patvaļīga un radīt negatīvas sekas personām. Kā ir atklāts vairākos ANO ziņojumos, ir pierādīts, ka personu (bieži vien žurnālistu, aktīvistu, opozīcijas pārstāvju, kritiķu un citu personu, kas izmanto savas tiesības uz vārda brīvību) novērošana noved pie patvaļīgas aizturēšanas, dažkārt pat spīdzināšanas un, iespējams, arī slepkavības bez tiesas.[89] Daudzās valstīs nav atbilstošu tiesību aktu vai arī tie netiek piemēroti, ir vājas procesuālās garantijas un neefektīva uzraudzība, un tas viss ir veicinājis atbildības trūkumu par nelikumīgu digitālo novērošanu. Šāda novērošana ir attīstījusies, vāji kontrolējot eksportu un tehnoloģiju nodošanu valdībām, kas īsteno plaši zināmas represijas politikas.

Turklāt šādu prettiesisku novērošanu netiešā veidā veicina un atbalsta ASV, kā arī citu demokrātisku valstu tehnoloģiju uzņēmumi, kas izstrādā un pārdod novērošanas tehnoloģijas valdībām, kuras tās savukārt izmantotu pret žurnālistiem, opozīcijas līderiem, aktīvistiem un citiem sabiedrības pārstāvjiem, kuriem ir nozīmīga loma demokrātiskā sabiedrībā. 2020. gada novembrī Eiropas Parlaments un Padome vienojās par jaunu tiesisko regulējumu, lai kontrolētu un ierobežotu tādu kibernovērošanas preču eksportu uz autoritāriem un represīviem režīmiem, kas ļauj "slēpti novērot fiziskas personas, novērojot, iegūstot, vācot vai

88 Sk., piemēram, UNODC. (2009). Current practices in electronic surveillance in the investigation of serious and organized crime. https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf

89 UN Human Rights Council. (2019). Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. https://digitallibrary.un.org/record/3814512#record-files-collapse-header

analizējot datus, tostarp biometriskos datus", un nepieļautu, ka šīs tehnoloģijas tiek izmantotas pretrunā ar cilvēktiesībām.[90]

Gan starptautiskā, gan nacionālā līmenī ir bijuši ilgstoši centieni regulēt valstu novērošanas pasākumus, ieviešot nepieciešamās aizsardzības garantijas, un izveidot regulējumu, lai nodrošinātu šādu pasākumu samērīgumu un atbilstību pamattiesībām. Demokrātiskās tiesiskās valstīs, lai veiktu mērķtiecīgu novērošanu noziedzīgu nodarījumu atklāšanas un izmeklēšanas interesēs, ir jāievēro stingri procesuālie noteikumi, to skaitā iepriekš jāsaņem tiesneša atļauja šādai novērošanai, lai nodrošinātu, ka personu tiesības netiek nesamērīgi ierobežotas vai pārkāptas. Tomēr, ja attiecībā uz tradicionālo novērošanu, kas tiek veikta noziedzīgu nodarījumu novēršanas un atklāšanas nolūkā, tas ir pamatā izdevies, tad daudz grūtāk ir vienoties par regulējumu un robežām masveida novērošanas pasākumiem, it īpaši tādiem, kas balstās uz mākslīgo intelekta sistēmu izmantošanu.

Masveida digitālā novērošana atšķiras no tradicionālās jeb mērķtiecīgās novērošanas. Tā ir sistemātiska cilvēku darbību un komunikācijas novērošana, kas īstenota, izmantojot informācijas un komunikācijas tehnoloģijas. Valstu veiktās masveida jeb stratēģiskās novērošanas galvenais mērķis ir proaktīvi identificēt "riskantas grupas", proti, tās mērķis ir identificēt iespējamas briesmas, nevis izmeklēt zināmus draudus. Masveida novērošanu var veikt arī tad, ja nepastāv aizdomas pret konkrētu personu vai personām.[91] Novērošana bieži vien ir saistīta ar personiskas informācijas iegūšanu un analīzi. Tā var ietvert dažādus personas dzīves aspektus, komunikāciju, informāciju par ceļošanu, finansiālo informāciju, darbībām internetā.

Eiropas Padome ir norādījusi, ka "pilsoņu masveida novērošana saskaņā ar ECTK ir pieļaujama tikai tad, ja tā ir absolūti jeb stingri nepieciešama demokrātisku institūciju aizsardzībai. Ņemot vērā, ka tā ievērojami apdraud ECTK nostiprinātās pamattiesības uz privātumu un vārda brīvību, dalībvalstīm ir jānodrošina, ka līdz ar novērošanas metožu attīstību, kā rezultātā notiek masveida datu

90 Stolton, S. (10 November 2020). EU to restrict sale of cyber-surveillance goods to repressive regimes. *EURACTIV.* https://www.euractiv.com/section/digital/news/eu-to-restrict-sale-of-cyber-surveillance-goods-to-repressive-regimes/; sk. arī Eiropas Parlamenta 2021. gada 25. marta normatīvo rezolūciju par priekšlikumu Eiropas Parlamenta un Padomes regulai, ar ko izveido Savienības režīmu divējāda lietojuma preču eksporta, pārvadājumu, starpniecības, tehniskās palīdzības un tranzīta kontrolei (pārstrādāta redakcija). https://www.europarl.europa.eu/doceo/document/TA-9-2021-0101_LV.html

91 Council of Europe. (2018). Mass Surveillance. https://rm.coe.int/factsheet-on-mass-surveillance-june2018-docx/16808b3dd8

vākšana, vienlaikus tiek izstrādāti arī tiesiski aizsardzības pasākumi, kas nodrošina cilvēka cieņas ievērošanu."[92]

Vai valstīm ir nepieciešams veikt masveida novērošanu, lai iedzīvotāji varētu būt drošībā? Par šo jautājumu ir ilgstoši diskutējuši cilvēktiesību aizstāvji, kā arī starptautiskās organizācijas un tiesas. Vēl vairāk šis jautājums ir kļuvis aktuāls līdz ar jauno tehnoloģiju, it īpaši sejas atpazīšanas un citu biometrisko tehnoloģiju, izmantošanu masveida novērošanai, ņemot vērā, ka tās rada vēl ievērojamāku apdraudējumu cilvēktiesībām.

AI HLEG vērš uzmanību, ka uzticama mākslīgā intelekta sasniegšanai ir svarīgi skaidri definēt, vai, kad un kā mākslīgo intelektu var izmantot, lai automātiski identificētu cilvēkus, un nošķirt personas identificēšu no tās izsekošanas, kā arī mērķtiecīgu novērošanu no masveida novērošanas.[93]

Eiropas Parlamenta piedāvātajā Priekšlikumā Eiropas Parlamenta un Padomes Regulai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrādes, ieviešanas un izmantošanas ētikas principiem tika norādīts, ka biometrisko datu izmantošana un vākšana attālinātās identifikācijas nolūkos publiskās vietās, izmantojot biometrisko vai sejas atpazīšanu, īpaši apdraud pamattiesības un ka dalībvalstu publiskās iestādes tās var ieviest vai izmantot, tikai ja tas ir nepieciešams, lai sasniegtu būtiskas sabiedrības intereses.[94]

Mākslīgā intelekta sistēmu izmantošana rada būtisku apdraudējumu, kas pamato nepieciešamību tās stingrāk regulēt un pat konkrētos gadījumos aizliegt to izmantošanu, lai nepieļautu, ka valsts iestādes tās mēģina ieviest, nepamatoti atsaucoties uz būtisku sabiedrības interešu aizsardzību. Šie jautājumi sīkāk apskatīti grāmatas turpmākajās nodaļās. Savukārt šīs nodaļas turpinājumā atklāts, kā valstis bieži vien nepamatoti kā argumentu izmanto nacionālās un sabiedrības drošības intereses, lai ieviestu masveida novērošanas pasākumus.

1.1.3.4. Drošība kā pamats valsts novērošanai

Masveida novērošanas pasākumus valstis ir ieviesušas pamatā ar mērķi novērst arvien pieaugošos draudus valsts un sabiedrības drošībai, it sevišķi, lai cīnītos pret terorismu. Pēc 2001. gada 11. septembra teroristu uzbrukumiem ASV sāka izmantot savu varu, lai veiktu masveida elektronisko novērošanu un sakaru pārtveršanu gan no ASV, gan citām pasaules valstīm. ASV masveida novērošanas prakse ir pamatā diviem EST nolēmumiem, kas tika pieņemti 2015. gadā "Schrems I" lietā un 2020. gadā "Schrems II" lietā. Ar šiem nolēmumiem par spēkā neesošiem

92 Council of Europe. (2018). Mass Surveillance. https://rm.coe.int/factsheet-on-mass-surveillance-june2018-docx/16808b3dd8

93 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

94 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

divas reizes tika atzīti Eiropas Komisijas lēmumi par aizsardzības līmeņa pietiekamību datu nodošanai uz ASV, kas veidoja pamatu datu nodošanai no ES uz ASV. Eksteritoriālās digitālās masveida novērošanas atklāšana ir sagrāvusi uzticību transatlantiskajām attiecībām un radījusi jautājumus arī par citu ilgtermiņa līgumu, kas paredz datu nodošanu starp ASV un ES, likumību, tostarp par Teroristu finansēšanas izsekošanas programmas nolīguma[95] un Pasažieru datu reģistra nolīguma[96] īstenošanu.

ES arī ir ieviesusi masveida novērošanas pasākumus drošības interešu vārdā. Nepieciešamība cīnīties pret terorismu ir novedusi pie datu saglabāšanas shēmu ieviešanas, kas paredz apmaiņu ar izlūkdienestu informāciju, masveida datu vākšanu un liela mēroga datubāzu izveidi ES, un tas viss veido nozīmīgu daļu no ES pretterorisma politikas. Nepieciešamība apkarot terorismu bija pamatā ES datu saglabāšanas režīmu ieviešanai, kas ļāva dalībvalstīm uzraudzīt elektroniskos sakarus drošības nolūkos. Kā steidzamu pretterorisma pasākumu, reaģējot uz teroristu uzbrukumiem 2004. gadā Madridē un 2005. gadā Londonā, ES pieņēma Datu saglabāšanas direktīvu[97]. Lai gan bija izteiktas bažas, ka šāda masveida novērošanas pasākuma ieviešana neatbilst pamattiesībām, tomēr, ņemot vērā milzīgo politisko spiedienu, direktīva tika ātri pieņemta un stājās spēkā 2006. gadā. Datu saglabāšanas direktīva pieprasīja dalībvalstīm uzlikt telekomunikāciju un interneta pakalpojumu sniedzējiem pienākumu saglabāt konkrētu kategoriju datus par mobilo un fiksēto telefonu sarunām un lietotāju atrašanās vietu, piekļuvi internetam un e-pasta lietošanu, kas neietver komunikācijas saturu, bet metadatus saglabāt vismaz sešus mēnešus un ne ilgāk kā divus gadus, un pēc pieprasījuma tos darīt pieejamus tiesībaizsardzības iestādēm smagu noziegumu un terorisma izmeklēšanas, atklāšanas un kriminālvajāšanas nolūkos. 2014. gadā EST pieņēma sprieduma apvienotajās lietās "Digital Rights Ireland" un "Seitlinger u. c.", ar kuru pasludināja Datu saglabāšanas direktīvu par spēkā neesošu, atzīstot, ka tā rada nepamatotu iejaukšanos pamattiesībās.[98]

95 Nolīgums starp Eiropas Savienību un Amerikas Savienotajām Valstīm par tādu finanšu ziņojumapmaiņas datu apstrādi un nodošanu, kurus Eiropas Savienība dara pieejamus Amerikas Savienotajām Valstīm, lai īstenotu Teroristu finansēšanas izsekošanas programmu. OV L 8, 13.01.2010. (spēkā līdz 31.10.2010.).

96 Nolīgums starp Amerikas Savienotajām Valstīm un Eiropas Savienību par pasažieru datu reģistra datu izmantošanu un pārsūtīšanu Amerikas Savienoto Valstu Iekšzemes drošības departamentam. *OV L* 215, 11.8.2012.

97 Eiropas Parlamenta un Padomes Direktīva 2006/24/EK (2006. gada 15. marts) par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK. *OV L* 105, 13.04.2006. (spēkā līdz 03.05.2006.).

98 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C293/12 .. Eiropas Savienības Tiesas prakse atsevišķi analizēta darba piektajā nodaļā.

EST ir izskatījusi daudzas lietas par elektronisko datu saglabāšanas režīmiem. 2020. gada oktobrī EST pieņēma nolēmumus, kuros izvērtēja Apvienotās Karalistes, Francijas un Beļģijas "liela apjoma" jeb masveida datu vākšanas vai saglabāšanas režīmu valsts drošības kontekstā atbilstību privātuma garantijām saskaņā ar ES tiesībām.[99] EST ir atzinusi, ka policijai un izlūkošanas iestādēm ir ļoti svarīga loma mūsu drošības garantēšanai, tomēr tām ir jādarbojas saskaņā ar noteiktām garantijām, lai novērstu to ļoti ievērojamās varas ļaunprātīgu izmantošanu. Tām būtu jākoncentrējas uz efektīvu un mērķtiecīgu novērošanas sistēmu nodrošināšanu, kas aizsargā gan mūsu drošību, gan pamattiesības. Demokrātiskā sabiedrībā neviena valsts varas iestāde nevar būt augstāka par likumu un ir jānosaka ierobežojumi un kontrole policijas un izlūkošanas iestāžu novērošanas pilnvarām.

Latvijas tiesību zinātnieks un bijušais Latvijas Republikas Satversmes tiesas tiesnesis asociētais profesors Uldis Ķinis uzsver, ka "demokrātiskā un tiesiskā valstī drošība iespējama tikai tad, ja sabiedrībā tiek garantētas cilvēktiesības un ievēroti vispārīgie tiesību principi".[100]

Līdzās regulējumam, kas saistīts ar elektroniskās komunikācijas saglabāšanas režīmiem, kritiku ir izraisījuši arī citi ES tiesību akti, kas paredz masveida datu saglabāšanu. Ļoti pretrunīgi vērtēta ir ES pasažieru datu reģistra sistēma, kas bija ES politikas reakcija uz traģiskajiem teroristu uzbrukumiem visā pasaulē un Eiropā, īpaši Parīzē un Briselē, kā arī pasažieru datu nolīgumi ar trešajām valstīm, tostarp ASV un Austrāliju. 2017. gadā EST secināja, ka ES un Kanādas Pasažieru datu reģistra nolīgums neatbilst Eiropas Savienības Pamattiesību hartas (Harta) 7. un 8. pantā noteiktajām tiesībām uz privātumu un datu aizsardzību. Ir kritizēti arī priekšlikumi regulai par personas apliecību un citu dokumentu drošības uzlabošanu, kas paredz biometrisko datu apstrādi[101], regulai, ar ko groza vīzu informācijas sistēmu[102], u. c. Tomēr ES līmenī pieņemtie pasākumi tiek daudz rūpīgāk izvērtēti un uzraudzīti nekā pasākumi, ko pieņem valstis nacionālā līmenī, īpaši saistībā ar lielo datu un jauno tehnoloģiju sniegtajām iespējām.

99 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C511/18 *La Quadrature du Net* u. c., C-512/18 *French Data Network* u. c. un C-520/18 *Ordre des barreaux francophones et germanophone* u. c., ECLI:EU:C:2020:791.

100 Ķinis, U. Kiberdrošība – tiesiski aizsargājama vērtība. *Jurista Vārds.* 06.10.2020., Nr. 40.

101 Eiropas Datu aizsardzības uzraudzītājs. (2018). Eiropas Datu aizsardzības uzraudzītāja atzinuma kopsavilkums par priekšlikumu regulai par Savienības pilsoņu personas apliecību un citu dokumentu drošības uzlabošanu. https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_summary_lv_0.pdf

102 FRA. (2018). The revised Visa Information System and its fundamental rights implications. https://fra.europa.eu/en/opinion/2018/visa-system

Dažādus uzraudzības pasākumus drošības interesēs plaši ievieš gan ES, gan atsevišķas valstis. Sākoties Covid-19 pandēmijai 2020. gadā, mēs varējām sekot līdzi neskaitāmiem piemēriem, kad valstis ieviesa jaunus masveida novērošanas pasākumus. Tie aplūkoti atsevišķi nodaļas turpinājumā.

Teroristu uzbrukumu draudi ir bieži izmantots arguments, lai pamatotu jaunu novērošanas pasākumu, tostarp mākslīgā intelekta novērošanas tehnoloģiju, izmantošanu. Piemēram, tūlīt pēc asiņainajiem uzbrukumiem Francijas pilsētā Nicā 2020. gada oktobrī, kuru laikā ar nazi tika nogalināti vairāki cilvēki, politiķi, to skaitā prezidenta Emanuela Makrona (*Emmanuel Macron*) valdības ministrs, aicināja izmantot mākslīgā intelekta sejas atpazīšanas tehnoloģijas, piemēram, sabiedriskajā transportā, lai veiktu iespējamo uzbrucēju novērošanu un novērstu turpmāku vardarbību un terorismu. Pirms gada, 2019. gada oktobrī, Nicā jau tika veikti eksperimenti, izvietojot sejas atpazīšanas kameras pie vidusskolas ieejas, bet tie tika pārtraukti pēc Francijas datu aizsardzības iestādes CNIL (*Commission Nationale de l'Informatique et des Libertés*) iejaukšanās. Sejas atpazīšanas tehnoloģiju izvietošana sabiedriskās vietās tika atzīta par nevajadzīgu un nesamērīgu, lai sasniegtu to noteikto mērķi – drošību. Pēc uzbrukumiem šis uzraudzības iestādes viedoklis tika kritizēts.

Nacionālās un sabiedrības drošības garantēšana vienmēr ir bijis neapstrīdams arguments, lai iedzīvotājus, kas dzīvo bailēs par savu drošību, varētu pārliecināt, ka novērošanas tehnoloģijas ir nepieciešamas viņu aizsardzībai. Līdzšinējā prakse rāda, ka masveida komunikācijas novērošanas pasākumi, kas tika ieviesti ar mērķi aizsargāt valsts un sabiedrības drošību, ir izrādījušies neefektīvi terorisma apkarošanai.[103] Tomēr, ja uz spēles tiek likta drošība, citi argumenti, piemēram, personu pamattiesību aizsardzība, vienmēr liksies mazāk svarīgi.

Saskaroties ar drošības apdraudējumu, valstīm vienmēr ir bijusi vēlēšanās strauji ieviest jaunus uzraudzības pasākumus, bet vēl vairāk šo tendenci ir ietekmējušas jauno tehnoloģiju radītās iespējas. Turpinājumā atklāts, kādā veidā jaunās tehnoloģijas ir ievērojami palielinājušas novērošanas praksi, radot jaunus būtiskus izaicinājumus, kam ir jāmeklē risinājumi.

103 Vinocur, N. (30 October, 2020). French politicians urge deployment of surveillance technology after series of attacks. *POLITICO.* https://www.politico.eu/article/french-politicians-urge-deployment-of-surveillance-technology-after-series-of-attacks/

1.2. Mākslīgā intelekta novērošanas tehnoloģijas

1.2.1. Mākslīgais intelekts kā "degviela" valsts novērošanai

Mākslīgā intelekta tehnoloģiju straujā attīstība ievērojami veicina jaunu novērošanas pasākumu ieviešanu un izmantošanu. Tās ļauj masveida novērošanu veikt ievērojami plašāk, detalizētāk un precīzāk analizēt dažādas īpašības un pazīmes daudzās jomās un dažkārt arī iepriekš nenojaustiem mērķiem. Šādu novērošanu var saukt par "gudro uzraudzību" (*smart surveillance* – angļu val.), uzsverot, ka šie jaunie risinājumi ir "inteliģenti" tādā nozīmē, ka tie, šķiet, mācās no novērotajiem datiem, kā arī paši "pieņem lēmumus", balstoties uz noteiktiem algoritmiem.

Mākslīgais intelekts uzlabo tiesībaizsardzības, drošības un izlūkošanas iestāžu novērošanas iespējas. Šīs iestādes sistemātiski ir izmantojušas datu analīzi, lai veiktu prognozēšanu, profilēšanu un preventīvu novērošanu. Mašīnu mācīšanās un dziļās mācīšanās algoritmi ievērojami veicina novērošanas iespējas. Tie rada jaunas tehnoloģiskās iespējas lielo datu kopu izveidei, apstrādei un izmantošanai unikālos un neizpētītos veidos, lai veiktu izvērtēšanu un prognozes par cilvēkiem, bieži vien bez pierādījumiem par to saistību ar noziedzību. Turklāt mākslīgā intelektā balstītas tehnoloģijas nebūt nav nekļūdīgas.

Arvien vairāk valstu novērošanas vajadzībām izmanto mākslīgā intelekta tehnoloģijas – sejas atpazīšanas sistēmas, viedās pilsētas platformas, viedo policiju, automatizētās robežkontroles sistēmas. Kārnegija Starptautiskā miera fonda (*Carnegie's Endowment for International Peace*) pētnieka Stīvena Feldšteina (*Steven Feldstein*) 2019. gada septembrī publicētais pētījums parādīja, ka vismaz 75 no 176 pasaules valstīm aktīvi izmanto mākslīgā intelekta tehnoloģijas novērošanas vajadzībām. Pētījums atklāj, ka 56 valstis ir ieviesušas viedās pilsētas jeb drošas pilsētas platformas, 64 valstis – sejas atpazīšanas sistēmas un 52 valstis – viedo tiesībaizsardzību (*smart policing* – angļu val.).[104] Šis skaits strauji palielinās, jo arvien vairāk valstu ievieš mākslīgā intelekta novērošanas tehnoloģijas.

It sevišķi valstis ar autoritārām sistēmām un zemu politisko tiesību līmeni iegulda daudz līdzekļu mākslīgā intelekta novērošanas sistēmās. Ķīna ir galvenais mākslīgā intelekta novērošanas virzītājspēks visā pasaulē. Modernas analītiskās sistēmas, sejas atpazīšanas kameras un sarežģītas novērošanas sistēmas iegādājušās daudzas Persijas līča, Austrumāzijas, Dienvidāzijas un Centrālāzijas valdības. Bet arī liberālās demokrātiskās Eiropas valstis arvien plašāk ievieš sejas atpazīšanas sistēmas, automatizētas robežkontroles sistēmas, prognozēšanas sistēmas tiesībaizsardzības nolūkos un drošas pilsētas sistēmas.

Mākslīgā intelekta novērošanas tehnoloģijas, kas vāc un apstrādā biometriskos datus, rada jauna veida būtisku apdraudējumu cilvēktiesībām. Pēdējie gadi

104 Feldstein (2019), The Global Expansion of AI surveillance.

iezīmē pagrieziena punktu, kad varam novērot arvien plašāku biometrisko datu izmantošanu, un šī tendence turpina tikai palielināties. Turpmāk arvien straujāk pieaugs mākslīgā intelekta sistēmu izstrādes, ieviešanas un izmantošanas rezultātā iegūtu biometrisko datu ģenerēšana un izmantošana.

Visplašākās diskusijas un kritika visā pasaulē ir par sejas atpazīšanas tehnoloģijām, kas vāc un izmanto biometriskos datus attālinātās identifikācijas nolūkos sabiedriskās vietās. Dažkārt tiesībaizsardzības iestādes un policija sejas atpazīšanas tehnoloģijas izmanto arī kā prognozēšanas rīku, kas analizē un izvērtē iedzīvotāju uzvedību. Šo novērošanas tehnoloģiju izmantošana aplūkota nodaļas turpinājumā.

1.2.2. Sejas atpazīšanas tehnoloģijas

Cilvēku spēja paust emocijas, tostarp ar sejas izteiksmes palīdzību, ir ļāvusi mums kā sabiedriskām būtnēm savā starpā komunicēt. Gadsimtiem tā ir bijusi arī iedvesmas avots neskaitāmiem izciliem mākslas darbiem. Atliek vien atcerēties slepeno smaidu Leonardo da Vinči (*Leonardo da Vinci*) slavenajā gleznā "Mona Liza". Tomēr mūsdienās mākslīgā intelekta pasaulē ir parādījušies jauni, daudz mazāk iedvesmojoši un emocionāli tās izmantošanas veidi. Cilvēka seja ir kļuvusi par datu avotu, ko izmanto gan valsts iestādes, gan privātie uzņēmumi, izstrādājot un ieviešot jaunas tehnoloģijas, veidojot novērošanas sabiedrību.

Mūsu sejas attēls, ar kuru mēs vienmēr esam varējuši brīvi rīkoties un kas ļauj mums sazināties, paust emocijas un iekšējās izjūtas dažādās situācijās, vai tās būtu prieks, sajūsma, pārsteigums, aizrautība, pateicība vai arī vienaldzība, neizpratne, bēdas, nožēla, dusmas, vienmēr ir piederējis tikai mums pašiem. Tomēr tagad arvien nenovēršamāk tas tiek izmantots, lai izstrādātu un ieviestu mākslīgā intelekta tehnoloģijas, veidotu datubāzes un trenētu algoritmus.

Sejas atpazīšana ir biometriska tehnoloģija, kas izmanto algoritmus un mašīnmācīšanos, lai identificētu personas no fotoattēla vai video. Tā ļauj salīdzināt digitālos sejas attēlus, lai noskaidrotu, vai tā ir viena un tā pati persona. Sejas atpazīšanas tehnoloģija ļauj, piemēram, tiesībaizsardzības iestādēm identificēt personas, salīdzinot viņu attēlus, kas uzņemti ar videonovērošanas kamerām, kuras uzstādītas sabiedriskās vietās, ar biometriskiem attēliem, kuri glabājas informācijas tehnoloģiju sistēmās.

Sejas atpazīšanas sistēmas izmanto skaitļošanas algoritmus, parasti mašīnmācīšanās modeļus, lai atlasītu unikālas personas sejas identifikācijas detaļas. Sejas atpazīšanas procesā ir vairāki soļi ar trim pamatdarbībām: sejas noteikšanu, sejas fiksēšanu un sejas salīdzināšanu. Pirmais solis ir sejas attēla uzņemšana, to nofotografējot vai nofilmējot. Attīstītas tehnoloģijas ļauj atpazīt sejas pūlī vai pat pēc kāda silueta. Otrais solis ir sejas ģeometrijas nolasīšana, izmantojot

sejas atpazīšanas programmatūru. Galvenie faktori ietver attālumu starp acīm un attālumu no pieres līdz zodam. Rezultāts ir "individuāls paraksts". Šis paraksts, kas faktiski ir matemātiska formula, pēc tam tiek salīdzināts ar zināmiem sejas attēliem datubāzē. Pamatojoties uz uzņemtā modeļa un atrasto datu līdzību, var noteikt atbilstību starp novērošanas kameras uzņemto attēlu un konkrēto sejas attēlu datubāzē. Neatkarīgi no paredzētā mērķa apstrādes darbības, ko veic šāda veida tehnoloģija, ir gandrīz vienādas.[105]

Sejas atpazīšanas tehnoloģijas arvien plašāk ievieš un izmanto dažādiem mērķiem gan valsts iestādes, gan privātie uzņēmumi. Sejas atpazīšana kā biometriskās autentifikācijas tehnoloģija ir izmantota jaunākajos viedtālruņos, ļaujot to lietotājiem atbloķēt savas ierīces, un dažas bankas to izmanto darījumu autorizēšanai. ASV, kā arī Eiropas lidostās tiek ieviestas un testētas sejas atpazīšanas sistēmas pasažieru identitātes pārbaudei, lai paātrinātu iekāpšanu, kā arī tās tiek izmantotas, lai piedāvātu pasažieriem personalizētus pakalpojumus.[106] Ne tikai privātie uzņēmumi, bet arī valstis ir sākušas izmantot sejas atpazīšanas tehnoloģiju identitātes pārbaudei. 2020. gada rudenī Singapūra paziņoja, ka būs pirmā valsts, kas sejas atpazīšanu izmantos personu identitātes pārbaudei.[107]

Sejas atpazīšanas sistēmas ir ieviesuši arī daudzi lielie sociālo mediju uzņēmumi, izraisot skaļus protestus. "Facebook" ieviesa sejas atpazīšanu, kas nosaka cilvēku vārdus augšupielādētās fotogrāfijās. ASV Ilinoisas štata iedzīvotāji iesniedza prasību tiesā pret "Facebook" par biometrisko datu apstrādi bez viņu piekrišanas. Lai izbeigtu tiesvedību, pamatojoties uz vienošanos, "Facebook" piedāvāja

105 Sejas atpazīšanas sistēma veic šādas datu apstrādes darbības:
a) attēlu iegūšana: indivīda sejas attēla uzņemšana un pārveidošana par digitālu attēlu;
b) sejas attēla noteikšana: sejas attēla noteikšana digitālajā attēlā un zonas marķēšana;
c) normalizēšana: lai izlīdzinātu noteikto sejas reģionu variācijas, piemēram, attēla pārveidošana standarta izmērā vai pat krāsu sadalījumu pagriešana vai izlīdzināšana;
d) atribūtu iegūšana (pazīmes): lai izolētu un izveidotu atkārtojamus rādījumus, kas atšķiras no indivīda digitālā attēla. Atribūtu kopa ir definēta kā veidne salīdzinājumiem ar sejas datubāzi – sejas parakstu;
e) glabāšana: ja indivīda seja tiek uzņemta pirmo reizi, attēlu un/vai atsauces modeli var saglabāt kā ierakstu turpmākiem salīdzinājumiem;
f) salīdzinājums: līdzības noteikšana starp paraugu un citu sistēmā iepriekš iekļautu modeli. Šo salīdzinājumu var veikt: 1) identifikācijai, 2) autentifikācijai vai pārbaudei un/vai 3) kategorizācijai.
Moraes, T. G., Almeida, E. C., de Pereira, J. R. L. (2021). Smile, You Are Being Identified! Risks and Measures for the Use of Facial Recognition in (Semi-)Public Spaces. *AI and Ethics, 1*, pp. 159–172. https://doi.org/10.1007/s43681-020-00014-3

106 Sk., piemēram, CNIL. (9 Octobre, 2020). Reconnaissance faciale dans les aéroports : quels enjeux et quels grands principes à respecter ? https://www.cnil.fr/fr/reconnaissance-faciale-dans-les-aeroports-quels-enjeux-et-quels-grands-principes-respecter

107 McDonald, T. (25 September, 2020). Singapore in world first for facial verification. *BBC News.* https://www.bbc.com/news/business-54266602

samaksāt 650 miljonus ASV dolāru.[108] Līdzīga prasība par biometrisko datu pretiesisku izmantošanu tika ierosināta arī pret "Instagram".[109] Tiesvedības ir ierosinātas arī pret tādiem tehnoloģiju milžiem kā "Microsoft", "Google" un "Amazon" par cilvēku attēlu izmantošanu bez piekrišanas, lai apmācītu tehnoloģijas.[110] Šīs tehnoloģijas tiek ieviestas arī iepirkšanās centros, lielveikalos, bibliotēkās un pat skolās, radot arī plašus protestus un pirmos datu uzraudzības iestāžu lēmumus, kas aizliedz to izmantošanu.[111]

Sejas atpazīšanas tehnoloģijas arvien plašāk izmanto arī policijas un citas tiesībaizsardzības iestādes ar mērķi garantēt sabiedrības drošību un cīnīties pret terorismu. Jau pieminētā Kārnegija Starptautiskā miera fonda pētnieka Stīvena Feldšteina 2019. gada septembrī publicētā aptauja liecina, ka vismaz 64 pasaules valstis novērošanas vajadzībām izmanto sejas atpazīšanas tehnoloģijas.[112] Tās tiek ieviestas visā pasaulē – ASV, Japānā, Singapūrā, Apvienotajos Arābu Emirātos, Krievijā, Ķīnā, kur mākslīgā intelekta novērošanas tehnoloģijas attīstītās visstraujāk, un daudzās citās valstīs. Simtiem pilsētu, lai cīnītos ar noziedzību, ir uzstādījušas kameras, kas aprīkotas ar sejas atpazīšanas tehnoloģijām, solot sniegt datus centrālajiem vadības centriem kā "drošas pilsētas" vai "gudras pilsētas" risinājumu. Visprogresīvākā šī tendence ir Ķīnā, kur 2019. gadā vairāk nekā 100 pilsētas iegādājās sejas atpazīšanas novērošanas sistēmas. Arī daudzas Eiropas valstis izstrādā un testē šīs tehnoloģijas sabiedriskās vietās drošības nolūkos, piemēram, Francija, Vācija, Spānija, Nīderlande un it īpaši Lielbritānija, un šo valstu skaits aizvien pieaug. Sabiedriskās organizācijas "AlgorithmWatch" 2019. gada pētījums liecina, ka no 27 ES dalībvalstīm vismaz 11 valstīs policijas iestādes izmanto sejas atpazīšanas tehnoloģijas, bet vēl astoņas plāno to ieviest nākamajos gados.[113] Šis skaits turpina pieaugt.

108 Moyer, E. (27 February, 2021). Facebook privacy lawsuit over facial recognition leads to $650M settlement. *Reuters.* https://www.reuters.com/article/us-facebook-privacy-lawsuit-idUSKCN25G08M

109 Holmes, A. (12 August, 2020). Instagram could face up to $500 billion in fines in class-action lawsuit alleging it illegally harvested biometric data. *Insider.* https://www.businessinsider.com/instagram-facing-500-billion-in-fines-in-facial-recognition-lawsuit-2020-8

110 Musil, S. (14 July, 2020). Amazon, Google, Microsoft sued over photos in facial recognition database. *CNET*. https://www.cnet.com/news/amazon-google-and-microsoft-sued-over-photos-in-facial-recognition-database/

111 EDPB (22 August, 2019), Facial recognition in school renders Sweden's ..; CNIL. (29 Octobre, 2019). Expérimentation de la reconnaissance faciale ..

112 Feldstein (2019), The Global Expansion of AI surveillance.

113 Kayser-Bril, N. (18 June, 2020). At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals. *Algorithm Watch.* https://algorithmwatch.org/en/face-recognition-police-europe/

Saraksti, kurus policija izmanto attēlu pārbaudei, var būt ļoti apjomīgi, un tajos var būt iekļauti cilvēki bez viņu ziņas. Džordžtaunas Universitātes Privātuma un tehnoloģiju centra Vašingtonā (*Center on Privacy and Technology at Georgetown University in Washington DC*) pētnieki 2016. gadā aprēķinājuši, ka aptuveni puse visu amerikāņu varētu atrasties tiesībaizsardzības iestāžu sejas atpazīšanas tīklos, jo daudzi štati ļauj policijai veikt meklēšanu autovadītāju apliecību datubāzēs.

2020. gada sākumā "The New York Times" atklāja, ka programmatūras uzņēmums "Clearview AI" Ņujorkā ir ieguvis miljardiem attēlu no sociālo mediju vietnēm un apkopojis tos sejas atpazīšanas datubāzē. Uzņēmums piedāvāja savus pakalpojumus policijai gan ASV, gan citām valstīm. Sociālo mediju platformas, piemēram, "Twitter", "Facebook" un "YouTube", pieprasīja "Clearview AI" pārtraukt iegūt attēlus no to vietnēm, norādot, ka tas pārkāpj viņu pakalpojumu sniegšanas noteikumus. Cilvēktiesību aizsardzības organizācijas pret uzņēmumu ir ierosinājušas vairākas tiesas prāvas gan Eiropā, gan ASV. Šāda tiesvedība tika ierosināta, piemēram, par Ilinoisas iedzīvotāju biometriskās informācijas – sejas attēlu – izmantošanu bez piekrišanas.[114]

2020. gada jūnijā arī Eiropas Datu aizsardzības kolēģija (*European Data Protection Board*) nāca klajā ar atzinumu, ka "Clearview AI" pakalpojums pārkāpj VDAR noteikumus.[115] "Clearview AI" paziņoja, ka ir pārtraucis šī pakalpojuma sniegšanu un attēlu meklētājprogramma darbojas likumu robežās. Zviedrijas datu uzraudzības iestāde 2021. gada februārī konstatēja, ka Zviedrijas Policijas pārvalde ir pārkāpusi datu aizsardzības noteikumus, izmantojot "Clearview AI" personu identificēšanai.[116]

"Clearview AI" nav vienīgais uzņēmums, kas ir ieguvis cilvēku seju attēlus šādā veidā. Polijas uzņēmumam "PimEyes" ir vietne, kas ikvienam ļauj atrast fotogrāfijas, un uzņēmums apgalvo, ka tā ir ieguvusi 900 miljonus attēlu, kaut arī, kā tā apgalvo, ne no sociālo mediju vietnēm. Savukārt "NtechLab" 2016. gadā izveidoja lietotni "FindFace", lai atļautu veikt sejas salīdzināšanu Krievijas sociālajā tīklā "VKontakte", kuras darbību vēlāk uzņēmums pārtrauca.[117]

114 Statt, N. (28 May 2020). ACLU sues facial recognition firm Clearview AI, calling it a 'nightmare scenario' for privacy. *The Verge.* https://www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws

115 EDPB. (10 June, 2020). Response to MEPs Sophie in 't Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI. https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en

116 EDPB (21 February, 2021), Swedish DPA ..

117 Roussi, A. (18 November, 2020). Resisting the rise of facial recognition. *Nature.* https://www.nature.com/articles/d41586-020-03188-2

Sejas atpazīšana galvenokārt tiek izmantota kriminālizmeklēšanā. Francijas pilsētā Lionā ar tās palīdzību tiek izmeklētas automašīnu zādzības. Īrijā to parasti izmanto, lai atklātu krāpniekus, kas pieprasa sociālos pabalstus, lietojot vairākas identitātes.[118] Pēdējos gados arvien izplatītāka kļūst automatizēta sejas atpazīšana reāllaikā (*live facial recognition* – angļu val.). Šo tehnoloģiju izmanto ne tikai pilsētu ielās, bet arī mūzikas koncertos, piemēram, Eda Šīrana (*Ed Sheeran*) koncertā, kā arī sporta sacensību laikā.[119] Gan ASV, gan Eiropā, piemēram, Itālijā, Vācijā, to izmanto pie futbola stadioniem, lai atrastu cilvēkus, kuri ir iekļauti vardarbīgu sporta līdzjutēju sarakstos.

Īpaši plaši reāllaika sejas atpazīšana tiek izmantota Apvienotajā Karalistē, kur ir ilga pieredze modernu novērošanas tehnoloģiju izmēģināšanā. Londonā pirmo reizi videonovērošanas sistēmas (CCTV) kameras policija uzstādīja 1953. gadā karalienes kronēšanas laikā un sāka pastāvīgi uzstādīt pagājušā gadsimta 60. gados. Londonā vēl nesen bija visvairāk novērošanas kameru uz vienu iedzīvotāju, ja salīdzina ar citām pasaules valstīm. Metropolitēna policijas dienests pirmo reizi izmantoja tehnoloģiju Notinghilas karnevālā 2016. gada augustā, un Dienvidvelsas policija pirmo reizi to izvietoja UEFA Čempionu līgas finālā 2017. gada jūnijā. Metropolitēna policijas dienests no 2016. gada līdz 2019. gadam veica desmit reāllaika sejas atpazīšanas testu sērijas, pārejot uz operatīvo izvietošanu 2020. gada sākumā. Dienvidvelsas policija to arī izmanto kopš 2017. gada galvenokārt lielos koncertos, festivālos un sporta pasākumos.[120] Abas policijas iestādes izmanto sejas atpazīšanu reāllaikā, konkrētā ierobežotā teritorijā un ierobežotu laika posmu, parasti izvietojot furgonu ar CCTV kamerām, izmantojot programmatūru, kas ļauj sejas attēlus no novērošanas saraksta salīdzināt ar seju attēliem, kas reāllaikā iegūti no CCTV plūsmas. Sejas atpazīšanas sistēma nav integrēta esošajās novērošanas sistēmās, piemēram, videonovērošanā.

2018. gadā Apvienotās Karalistes datu aizsardzības iestāde – Informācijas komisāra birojs (*Information Commissioner's Office*, ICO) – uzsāka izmeklēšanu pret abām policijas iestādēm par sejas atpazīšanas izmantošanu. 2020. gadā ICO publicēja ziņojumu, kurā vērsa uzmanību, ka policijas spēkiem ir "jāpiebremzē" un jāpamato šīs tehnoloģijas izmantošana. Tajā pašā laikā iestāde neaizliedza

118 Deegan, G. (11 September, 2018). Facial imaging software detects 28 cases of welfare fraud in 2018. *The Irish Times.* https://www.irishtimes.com/news/crime-and-law/facial-imaging-software-detects-28-cases-of-welfare-fraud-in-2018-1.3626076

119 Burgess, M. (4 September, 2019). UK police can use controversial facial recognition tech, court rules. *WIRED.* https://www.wired.co.uk/article/police-facial-recognition-south-wales-court-decision

120 Fussey, P., Murray, D. (2020). Policing Uses of Live Facial Recognition in the United Kingdom. In: Kak, A. (ed.), *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute, pp. 78–85. https://ainowinstitute.org/regulatingbiometrics.html

policijai izmantot šo tehnoloģiju, tikai norādīja uz prasībām, kuras nepieciešams ievērot. Tajā pašā laikā ICO arī norādīja, ka, cik ātri vien iespējams, ir jāpārskata esošais un jāpieņem jauns regulējums.[121]

ICO ziņojums tika publicēts pēc Augstākās tiesas sprieduma lietā, kurā tika izvērtēts, vai Dienvidvelsas policija, izmantojot sejas atpazīšanas sistēmas, nav pārkāpusi cilvēktiesības un datu aizsardzības prasības. Tiesa konstatēja, ka nav ievērotas vairākas prasības, piemēram, policija nebija veikusi saprātīgus pasākumus, lai noskaidrotu, vai programmatūra nerada rasu vai dzimumu aizspriedumus, lai gan tā bija jauna un pretrunīgi vērtēta tehnoloģija. Tajā pašā laikā tā atzina šīs tehnoloģijas izmantošanu par samērīgu un to neaizliedza, kā arī norādīja, ka nav nepieciešams pieņemt jaunu regulējumu, jo attiecībā uz to ir piemērojams esošais regulējums.[122]

Atšķirībā no Apvienotās Karalistes sejas atpazīšanas tehnoloģiju izmantošana policijas darbā ir aizliegta vairākās ASV pilsētās. 2019. gada maijā Sanfrancisko bija pirmā ASV pilsēta, kas aizliedza to izmantot policijas un valsts varas iestādēm. Drīz tai sekoja citas pilsētas – Oklenda, Somervila, Bostona, Kalifornija, Mineapolisa.[123] Visstingrāko aizliegumu ir piemērojusi ASV pilsēta Portlenda Oregonas štatā, kurā 2020. gada septembrī tika aizliegts sejas atpazīšanas tehnoloģijas izmantot gan valsts iestādēm, gan privātajiem uzņēmumiem.[124]

Interesanti, ka pat ASV tehnoloģiju uzņēmumi, kas iepriekš ir mēģinājuši visiem spēkiem izvairīties no saistoša regulējuma, paši ir sākuši pieprasīt šo tehnoloģiju regulējumu. 2020. gadā jūnijā "IBM" un "Amazon" ieviesa ierobežojumus sejas atpazīšanas tehnoloģiju pārdošanai pēc antirasisma protestiem visā pasaulē, reaģējot uz Džordža Floida (*George Floyd*) nāvi.[125] Tam sekoja "Microsoft" paziņojums, ka tas apturēs sejas atpazīšanas tehnoloģiju pārdošanu policijas iestādēm, vismaz līdz brīdim, kad būs pieņemts ASV federālais likums, kas regulēs šīs tehnoloģijas. "Microsoft" prezidents Breds Smits (*Bradford Lee Smith*) paziņoja, ka

121 ICO. (2019). ICO investigation into how the police use facial recognition technology in public places. https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

122 O'Donoghou, C., O'Brien, S. (17 August, 2020). Face-off part 2: UK Court of Appeal finds deficiencies in use of automated facial recognition technology. *Technology Law Dispatch.* https://www.technologylawdispatch.com/2020/08/in-the-courts/face-off-part-2-uk-court-of-appeal-finds-deficiencies-in-use-of-automated-facial-recognition-technology/

123 Lyons (13 February, 2021), Minneapolis prohibits use of facial recognition software ..

124 Peters, J. (9 September 2020). Portland passes strongest facial recognition ban in the US. *The Verge*. https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology

125 Karen, H. (June 12, 2020). The two-year fight to stop Amazon from selling face recognition to the police. *MIT Technology Review.* https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/

visiem tiesību aktiem, kas regulēs sejas atpazīšanu, jābūt stingri balstītiem uz cilvēktiesībām.[126] Tas, ka lielie tehnoloģiju uzņēmumi, kuriem galvenā interese vienmēr ir saistīta ar peļņas gūšanu, sāk pieprasīt no valdībām regulējumu, tiek skaidrots gan ar vēlēšanos novērst riskus, ko rada to tehnoloģijas, un veicināt uzticēšanos, gan ar iespēju tādējādi palielināt savu dominanci. Tajā pašā laikā tie tikai atkārto to, uz ko jau ilgstoši vērš uzmanību pētnieki, tiesību zinātnieki, cilvēktiesību aizstāvji, kā arī starptautiskās organizācijas.

Ne tikai ASV, bet arī ES arvien skaļāk tiek pausts satraukums par šīs tehnoloģijas izmantošanu tiesībaizsardzības iestāžu darbībā, par tās radītajiem būtiskajiem riskiem, kā arī arvien vairāk tiek uzsvērta nepieciešamība regulēt un pat pavisam aizliegt šo tehnoloģiju izmantošanu. Kamēr ES cenšas ātri izstrādāt jaunu mākslīgā intelekta regulējumu, kas noteiktu stingras prasības un ierobežojumus sejas atpazīšanas tehnoloģiju izmantošanai, īpaši aktīvi to pieprasa pilsoniskās sabiedrības organizācijas.

Daudzas cilvēktiesību aizstāvības organizācijas ir vērsušas uzmanību uz šo tehnoloģiju radīto apdraudējumu, arvien skaļāk pieprasot apturēt un aizliegt to izmantošanu. 2020. gada novembrī EDRi uzsāka kampaņu "Atgūsti savu seju!".[127] Divpadsmit cilvēktiesību organizācijas pieprasīja, lai Eiropas valstu iestādes uzklausa iedzīvotājus saistībā ar sejas atpazīšanas un citu biometrisko tehnoloģiju izmantošanu publiskās telpās. EDRi kampaņa aicināja aizliegt biometrisko masveida novērošanu, reaģējot uz tiesībaizsardzības un policijas iestāžu ātru un slepenu nelikumīgu šo tehnoloģiju ieviešanu daudzās Eiropas valstīs. Mēneša laikā tika savākti vairāk nekā 25 000 cilvēku paraksti. 2021. gada februārī EDRi uzsāka arī Eiropas pilsoņu iniciatīvas petīciju, lai aicinātu Eiropas Komisiju aizliegt sabiedriskās vietās izmantot biometriskās novērošanas tehnoloģijas, jo īpaši sejas atpazīšanu.[128] Nedēļas laikā to parakstīja 27 000 ES iedzīvotāju. Šīs iniciatīvas ir rezultāts dažādu valstu cilvēktiesību aizsardzības organizāciju ilgstošiem centieniem iebilst pret sejas atpazīšanas tehnoloģiju izmantošanu masveida novērošanai, tai skaitā protestu un demonstrāciju laikā, tomēr ar to var nepietikt, ja nesekos konkrētas likumdevēja darbības starptautiskā līmenī.

126 Greene, J. (11 June, 2020). Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM. *The Washington Post.* https://www-washingtonpost-com.cdn.ampproject.org/c/s/www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/?outputType=amp

127 SHARE Foundation, Hermes Center, Bits of Freedom, ARTICLE19, Homo Digitalis and EDRi. (12 November, 2020). *EDRi*. Campaign "Reclaim Your Face" calls for a Ban on Biometric Mass Surveillance. https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/

128 European Citizens' Initiative. Civil society initiative for a ban on biometric mass surveillance practices. https://reclaimyourface.eu

Viena no organizācijām, kas piedalās kampaņas rīkošanā, ir Itālijas organizācija "Hermeja centrs" (*Hermes Center*), kas sadarbojās ar "Wired Italia", lai veiktu izmeklēšanu, kuras laikā tika atklāts, ka Komo pilsētā mēnešiem ilgi bija uzstādīta un pārbaudīta sejas atpazīšanas sistēma. Centrs norādīja, ka, uzstādot sistēmu, netika nodrošināta pārredzamība un nebija skaidra tiesiskā regulējuma, kā arī pastāvēja bažas par privāto uzņēmumu lomu, īpaši "Huawei", šo tehnoloģiju ieviešanā. Pilsēta iztērēja valsts naudu sistēmai, kuru Itālijas Datu aizsardzības iestāde lūdza pārtraukt, norādot uz tās neatbilstību pamattiesībām.

EDRi kampaņā iesaistījusies arī Serbijas "SHARE Foundation". Belgradas Republikas laukumā pie sienas stiprinājumiem ir redzamas kupola formas kameras, kas nemanot skenē cilvēkus, kuri staigā pa centrālo laukumu. Tā ir viena no 800 vietām pilsētā, par kuru Serbijas valdība pagājušajā gadā paziņoja, ka to uzraudzīs, izmantojot kameras, kas aprīkotas ar sejas atpazīšanas programmatūru, kura tika iegādāta no Ķīnas uzņēmuma "Huawei". Valdība nejautāja Belgradas iedzīvotājiem, vai viņi šādas kameras vēlas. "SHARE Foundation", kuru vada Danilo Krivokapičs (*Danilo Krivokapic*) pēc neveiksmīgiem informācijas pieprasījumiem, apšaubot projekta likumību un efektivitāti, uzsāka pūļa finansētu sabiedrības kampaņu "Tūkstošiem kameru" (*Hiljade Kamera*), lai atklātu informāciju, identificētu un atzīmētu vietas ap Belgradu, kur tiek uzstādītas viedās novērošanas kameras ar sejas atpazīšanas programmatūru.[129]

Cilvēktiesību aizstāvības organizāciju mērķis ir pēc iespējas plašāk informēt sabiedrību par biometrisko novērošanas tehnoloģiju izmantošanu un to radīto apdraudējumu. Līdzās privātuma zaudēšanai to izmantošana var radīt aizspriedumus un diskrimināciju, kā arī nepamatotu apcietināšanu. Arvien vairāk pētījumu parāda, ka šīs tehnoloģijas nav precīzas un bieži kļūdās, it īpaši, ja tās izmanto attiecībā uz sievietēm, tumšādainiem cilvēkiem, bērniem un veciem cilvēkiem. Tiek arī pamatoti uzsvērts, ka tās ietver biometrisko datu apstrādi, kas rada būtiskus un šobrīd pat skaidri nenosakāmus drošības riskus.[130] Valdības var šīs tehnoloģijas izmantot protestētāju un opozīcijas apspiešanai, ierobežojot vārda, pulcēšanās un biedrošanās brīvību un tādējādi radot būtisku apdraudējumu tiesiskumam un demokrātijai. Šie apdraudējumi detalizētāk apskatīti nodaļas turpinājumā, pirms tam aplūkojot vēl divus mākslīgā intelekta novērošanas tehnoloģiju izmantošanas veidus.

129 Roussi (18 November, 2020), Resisting the rise of facial ..

130 Sk., piemēram, Doffman, Z. (14 August, 2019). New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report. *Forbes.* https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#76f9901046c6

1.2.3. Emociju uztveršanas tehnoloģijas

Mūsdienās ļoti ātri attīstās mākslīgā intelekta tehnoloģijas, kas tiek izmantotas, ne tikai lai atpazītu sejas, bet arī emocijas un dažādas citas īpašības un pazīmes, kas raksturo personas. Tas ir cieši saistīts ar pēdējos gados strauji pieaugošo tendenci izmantot biometriskās tehnoloģijas. Tās pamatā tiek izmantotas personu autentifikācijai jeb identitātes pārbaudei. Biometrisko tehnoloģiju lietošana tiek normalizēta ikdienā. Piemēram, pirkstu nospiedumi vai sejas atpazīšana tiek piedāvāta kā telefonu atbloķēšanas vai bankas maksājumu autentifikācijas līdzeklis. Biometrisko datu izmantošana autentifikācijā ir jānošķir no to izmantošanas citos nolūkos, piemēram, uzvedības analīzei un vērtēšanai, kas rada jaunus būtiskus apdraudējumus.[131]

Ja agrāk tehnoloģijas ļāva atbildēt uz jautājumu, kas ir konkrētais cilvēks, tad tagad jau tiek uzdots jautājums, kāds ir šis cilvēks?[132] Līdzās personu identificēšanai arvien vairāk tiek apgalvots, ka mākslīgā intelekta sistēmas no ķermeņa datiem spēj izsecināt demogrāfiskās īpašības, emocionālos stāvokļus un personības iezīmes. Mākslīgā intelekta sistēmas, piemēram, sejas atpazīšanas tehnoloģijas, arvien vairāk izmanto algoritmus, kas analizē emocijas, uzvedību, balsi, izteicienus, acu kustības, gaitu, ķermeņa reakciju u. tml.

Emociju uztveršanas sistēma ir mākslīgā intelekta sistēma, kuras mērķis ir identificēt vai izsecināt fizisku personu emocijas vai nodomus, pamatojoties uz viņu biometriskajiem datiem.[133] Emocionālais mākslīgais intelekts attiecas uz tehnoloģijām, kuras izmanto afektīvās skaitļošanas un mākslīgā intelekta metodes, lai nojaustu, uzzinātu un mijiedarbotos ar cilvēka emocionālo dzīvi.[134] Šīs tehnoloģijas tiek sauktas arī par uzvedības atpazīšanas (*behavior recognision* – angļu val.) tehnoloģijām.

Izšķir arī biometriskās kategorizācijas sistēmas, kas ir mākslīgā intelekta sistēmas, kuru mērķis ir noteikt fizisku personu piederību noteiktām kategorijām, piemēram, tādām kā dzimums, vecums, matu krāsa, acu krāsa, tetovējumi, etniskā izcelsme vai seksuālā vai politiskā orientācija, pamatojoties uz biometriskajiem datiem.[135]

Daudzi zinātnieki populārzinātniskās grāmatās ir norādījuši, ka mākslīgā intelekta un biotehnoloģiju saplūšana ir viens no nozīmīgākajiem nākotnes

131 Pauwels, E. (2020). Artificial Intelligence and data capture technologies in violence and conflict prevention. https://www.globalcenter.org/wp-content/uploads/2020/10/GCCS_AIData_PB_H.pdf

132 Kak, A. (ed.). (2020). *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute. https://ainowinstitute.org/regulatingbiometrics.html

133 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts, 3. panta 34. punkts.

134 Mcstay (2020), Emotional AI, Soft Biometrics and the Surveillance ..

135 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts, 3. panta 35. punkts.

izaicinājumiem cilvēcei. Zinātnieks Stīvens Hokings (*Stephen Hawking*) grāmatā "Īsas atbildes uz svarīgiem jautājumiem" (*Brief Answers to the Big Questions*), kuru gan viņš pats nepaguva pabeigt un kura tika publicēta jau pēc viņa nāves 2018. gadā, atzīst, ka jaunu tehnoloģiju, īpaši mākslīgā intelekta un biotehnoloģiju, attīstība rada jaunus pamattiesību riskus un apdraud demokrātiju.[136] Arī vēsturnieks un filozofs profesors Juvāls Noa Harari (*Yuval Noah Harari*) grāmatā "21 lekcija 21. gadsimtam" (*21 Lessons for the 21st century*) brīdina, ka informācijas tehnoloģiju un biotehnoloģiju revolūcija un saplūšana, kas ļauj lielo datu algoritmiem izprast mūsu domas un jūtas, tās kontrolēt un ar tām manipulēt, rada lielāko izaicinājumu, ko cilvēce ir jebkad piedzīvojusi.[137] Pēc Harari domām, iespējams, visbūtiskākā 21. gadsimta attīstības tendence ir "zem ādas" uzraudzība, kura rada iespēju pilnīgi izprast cilvēku, ievācot biometriskos datus un tos analizējot, un var ļaut uzzināt par cilvēku vairāk, nekā viņš zina pats par sevi.[138] Ja iepriekš valdības un uzņēmumi galvenokārt novēroja mūsu rīcību pasaulē – kur dodamies, ar ko satiekamies –, tad tagad tos vairāk interesē tas, kas notiek mūsu ķermenī – mūsu veselības stāvoklis, ķermeņa temperatūra un asinsspiediens. Šāda veida biometriskā informācija var atklāt par mums daudz vairāk nekā jebkad agrāk. Zinātnieks turklāt brīdina, ka Covid-19 pandēmija var būt nozīmīgs pagrieziena punkts novērošanas vēsturē, jo tā var "normalizēt" masveida novērošanas rīku ieviešanu valstīs, kuras līdz šim tos ir noraidījušas, kā arī tā liecina par dramatisku pāreju no "virs ādas" uz "zem ādas" novērošanu.[139]

Mākslīgā intelekta sistēmu izmantošana fizisku personu emocionālā stāvokļa noteikšanai apdraud cilvēktiesības un var radīt nozīmīgu kaitējumu indivīdiem. Tās tiek arvien plašāk izmantotas personu vērtēšanai dažādās jomās, ieskaitot izglītību un darba attiecības. Tās tiek izmantotas skolās, lai izvērtētu skolēnu sasniegumus. Tās tiek izmantotas darba intervijās un darbinieku vērtēšanā, lai noteiktu, kurš ir "produktīvāks" vai "labāks darbinieks", turklāt bieži vien pašus darbiniekus par to neinformējot.[140] ASV bankas izmanto šīs tehnoloģijas, lai varētu novērtēt, vai darbinieki pietiekami bieži smaida bankas apmeklētājiem.[141] Tehnoloģiju uzņēmumi nāk klajā ar arvien jaunām novērošanas ierīcēm, kas

136 Hawking, S. (2018). *Brief Answers to the Big Questions*. United States: Bantam, p. 186.

137 Harari, Y. N. (2018). *21 Lessons for the 21st Century*. New York: Spiegel & Grau.

138 Harari, Y. N. (20 March, 2020). Yuval Noah Harari: the world after coronavirus. *Financial Times* https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

139 Harari, Y. N. (2020). Yuval Noah Harari: "Every crisis is also an opportunity." *UNESCO Courier*, 2020-3. https://en.unesco.org/courier/2020-3/yuval-noah-harari-every-crisis-also-opportunity

140 Sk. Crawford, et al. (2019), AI Now 2019 Report.

141 Paresh, D., Jeffrey, D. (19 April, 2021). U.S. banks deploy AI to monitor customers, workers amid tech backlash. *Reuters.* https://www.reuters.com/technology/us-banks-deploy-ai-monitor-customers-workers-amid-tech-backlash-2021-04-19/

ļauj iegūt un analizēt lietotāju biometriskos datus. "Amazon" veselības aprocei "Halo" ir paredzēta izvēles funkcija, kas prasa, lai aproces lietotājs nofotografētu četras ķermeņa puses apakšveļā vai ādas drēbēs, un pēc tam tā ģenerē ķermeņa 3D modeli, kā arī izmanto mikrofonu un mašīnmācīšanos, lai analizētu lietotāja balsi, sniedzot ieskatu par to, kā cilvēki uztver lietotāja toni, piemēram, vai tas ir valdonīgs vai aizkaitināts.[142] Šo ierīču spējas ir ļoti ierobežotas, un to rezultāti nav ticami, taču tas ir labs veids, kādā uzņēmumi var iegūt visintīmākos datus un attīstīt savas tehnoloģijas tālāk.

Būtisku apdraudējumu rada novērošanas tehnoloģiju izmantošana arī valsts iestādēs. Piemēram, Kortreikā Beļģijā un Marveljā Spānijā vietējā policija izmantoja ķermeņa atpazīšanas tehnoloģiju, kas analizē personu gaitu un apģērbu. Tā ļauj arī atpazīt sejas, tomēr, lai šo funkciju ieslēgtu, tika gaidīta "zaļā gaisma" no uzraugošajām iestādēm.[143]

Plašu kritiku izraisīja ES finansētais projekts "iBorderCtrl", kas tika īstenots no 2016. līdz 2019. gadam. Tā mērķis bija izstrādāt automatizētu melu noteikšanas sistēmu, lai uzlabotu ES robežu kontroli. Projektā iesaistījās Ungārijas, Grieķijas, kā arī Latvijas drošības iestādes. Projekts paredzēja ieviest ieceļotāju kontroles sistēmu, kas darbotos šādi – ieceļotājs, kurš vēlas iekļūt ES, pirms ierašanās lidostā, izmantojot savu datoru, piesakās vietnē, augšupielādējot savas pases attēlu. Uz ekrāna parādās virtuāls policists tumši zilā formas tērpā. Viņš uzdod dažādus jautājumus, piemēram: "Kāds ir tavs uzvārds?", "Kāda ir tava pilsonība?", "Kāds ir tavs ceļojuma mērķis?" Ieceļotājs atbild uz uzdotajiem jautājumiem, un virtuālais policists izmanto tīmekļa kameru, lai skenētu viņa seju un acu kustības, lai noteiktu, vai tiek melots vai nē. Intervijas beigās sistēma piešķir kvadrātkodu, kas jāuzrāda apsargam robežkontrolē. Apsargs noskenē kodu, izmantojot planšetdatoru, noņem pirkstu nospiedumus un pārskata uzņemto sejas attēlu, lai pārbaudītu, vai tas atbilst pasei. Apsarga planšetdatorā tiek parādīts rezultāts 100 punktu skalā, kas parāda, vai mašīna ir atzinusi sacīto par patiesību. Ceļotājiem, kurus uzskata par bīstamiem, var liegt ieceļošanu ES.[144] Eiropas datu aizsardzības bijušais uzraudzītājs Džovanni Butarelli (*Giovanni Buttarelli*) vērsa uzmanību uz to, ka šī sistēma var diskriminēt cilvēkus viņu etniskās izcelsmes dēļ. Šāda veida sistēmas būtiski apdraud cilvēktiesības, īpaši diskriminācijas aizlieguma principu.

EDRi vērš uzmanību, ka mākslīgā intelekta testēšanai uz Eiropas robežām, lai it kā atklātu melus, izmantojot imigrācijas lietotnes, vai maldināšanu par angļu valodas testiem, izmantojot balss analīzi, trūkst ticama zinātniska pamatojuma.

142 Swisher, K. (27 November, 2020). Amazon wants to get even closer. Skintight. *The New York Times.* https://www.nytimes.com/2020/11/27/opinion/amazon-halo-surveillance.html

143 Kayser-Bril (18 June, 2020), At least 11 police forces use face recognition ..

144 Gallagher, Jona (26 July, 2019), We tested Europe's new lie detector for travelers ..

ES migrācijas politikā arvien lielāku nozīmi ieņem mākslīgā intelekta sistēmas, piemēram, sejas atpazīšana, algoritmiskās profilēšanas un prognozēšanas rīki, kas paredzēti izmantošanai migrācijas pārvaldības procesos, tostarp piespiedu izraidīšanai. Šie izmantošanas gadījumi var pārkāpt datu aizsardzības tiesības, tiesības uz privātumu, tiesības uz nediskrimināciju un vairākus starptautisko migrācijas tiesību principus, tostarp tiesības meklēt patvērumu.[145]

Kā norāda AI HLEG, mākslīgā intelekta tehnoloģiju izmantošana personu vērtēšanā rada būtisku pamattiesību apdraudējumu: "Jebkāda iedzīvotāju vērtēšana var novest pie patstāvības zaudējuma un apdraudēt nediskriminēšanas principu. Vērtēšana būtu jāizmanto tikai tad, ja tā ir pamatota un ja pasākumi ir samērīgi un taisnīgi. Valsts iestāžu vai privātā sektora veikta iedzīvotāju vērtēšana (vispārējs "morālās personības" vai "ētiskās godprātības" vērtējums) visos aspektos un plašā mērogā apdraud šīs vērtības, jo īpaši, ja to neizmanto saskaņā ar pamattiesībām vai ja to izmanto nesamērīgi, bez skaidri noteikta un paziņota leģitīmā mērķa. [..] Vēlams, lai, kad vien tas iespējams, tiktu piedāvāta iespēja izstāties no vērtēšanas mehānisma bez nelabvēlīgām sekām; citos gadījumos ir jāparedz vērtējuma apstrīdēšanas un labošanas iespējas. Tas ir īpaši svarīgi situācijās, kad pušu starpā pastāv varas asimetrija. Šādas atteikšanās iespējas ir jānodrošina tehnoloģijas izstrādes stadijā, kad tas ir vajadzīgs, lai garantētu atbilstību pamattiesībām, un ir nepieciešams demokrātiskā sabiedrībā."[146]

Mākslīgā intelekta tehnoloģiju izmantošana cilvēku vērtēšanai un uzvedības analizēšanai ir radījusi plašu kritiku ne tikai tāpēc, ka tā var atspoguļot dažādus aizspriedumus un būt diskriminējoša, bet arī tāpēc, ka trūkst zinātnisku pierādījumu, vai šādas tehnoloģijas var nodrošināt precīzus vai pat derīgus rezultātus. Ir apstrīdams zinātniskais pamats tehnoloģijām, kas apgalvo, ka, pamatojoties uz fizioloģiskiem mērījumiem, piemēram, sejas izteiksmi, balsi un gaitu, var atklāt tādas lietas kā personība, emocijas, garīgā veselība un citus iekšējos stāvokļus. Tāpēc tām nevajadzētu būt nozīmīgām svarīgu lēmumu pieņemšanā par cilvēka dzīvi, piemēram, darbinieku izvērtēšanā vai pieņemšanā darbā, apdrošināšanas cenu noteikšanā, pacientu sāpju novērtēšanā vai skolā skolēnu sasniegumu izvērtēšanā. Pilsoniskās sabiedrības organizācijas un zinātniskās institūcijas, piemēram, *AI Now* institūts, arvien skaļāk un pārliecinošāk mudina valdības aizliegt šo tehnoloģiju izmantošanu, īpaši tādu svarīgu lēmumu pieņemšanā, kas ietekmē cilvēku dzīvi un piekļuvi iespējām.[147]

145 EDRi (12 January, 2021), Re: Open letter: Civil society call for the introduction of red lines ..

146 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

147 Crawford, et al. (2019), AI Now 2019 Report.

Būtisku apdraudējumu rada arī šāda veida mākslīgā intelekta novērošanas tehnoloģiju izmantošana tiesībaizsardzības iestāžu un policijas darbā noziedzības prognozēšanai.

1.2.4. Prognozēšana tiesībaizsardzības nolūkā

Prognozēšana tiesībaizsardzības nolūkā (*predictive policing* – angļu val.) ir apzīmējums, kas balstās uz apgalvojumu, ka, izmantojot datu kopu algoritmisku apstrādi, var atklāt iespējamo likumpārkāpumu modeļus nākotnē, kurus tādējādi var novērst, pirms tie tiek īstenoti.[148] Lai gan prognozējošās tiesībaizsardzības pirmsākumi varētu būt meklējami datorizētas noziedzības kontroles eksperimentos 20. gadsimta 70. gados un prognozēšana noziedzības un soda jomā ir izstrādāta un apspriesta daudzus gadu desmitus, šis termins galu galā tika saistīts tieši ar lielajiem datiem.[149] Prognozēšana kā plaša tendence ir ievērojami ietekmējusi drošības jomas attīstību visā pasaulē, tai skaitā Eiropā un ASV.

Prognozēšanas metodes tiesībaizsardzības nolūkos var iedalīt četrās lielās kategorijās:

1) metodes, kuru mērķis ir prognozēt noziedzīgus nodarījumus vai prognozēt, kur un kad ir paaugstināts noziedzības risks;
2) metodes, kuru mērķis ir prognozēt likumpārkāpējus vai identificēt personas, kuras nākotnē var izdarīt likumpārkāpumu vai atkārtotu pārkāpumu;
3) metodes, kuru mērķis ir prognozēt vai izveidot profilus, kas ir līdzīgi iepriekšējo likumpārkāpēju profiliem, un
4) metodes, kuru mērķis ir prognozēt noziedzīgu nodarījumu upurus, lai identificētu grupas vai personas, kuras varētu kļūt par noziedzīga nodarījuma upuriem.[150]

Prognozēšanas metodes var iedalīt, balstoties arī uz algoritmisko datu vai izlūkošanas analīzes iespējamiem mērķiem tiesībaizsardzības iestāžu un policijas darbības kontekstā. Proti, ir iespējams izšķirt prognozēšanu tiesībaizsardzības nolūkos, kas iekļauj stratēģisko plānošanu, prioritāšu noteikšanu un prognozēšanu; operatīvās izlūkošanas sasaisti un novērtēšanu, kas savukārt var ietvert,

148 Wilson, D. (2018). Algorithmic patrol: the futures of predictive policing, p. 108. In: Zavrsnik, A. (ed.), *Big Data, Crime and Social Control. Routledge Frontiers of Criminal Justice*. Routledge, London, p. 108; sk. arī Gonzelez Fuster, G. (2020). Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf

149 Wilson (2018), Algorithmic patrol: the futures of predictive policing, p. 109.

150 Perry, W. L. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND.

piemēram, noziedzības novēršanas darbības, lēmumu pieņemšanu vai riska novērtēšanu attiecībā uz indivīdiem.[151]

Prognozējošā pieeja tiesībaizsardzībā bieži vien vismaz daļēji balstās uz tādu datu apstrādi, kas sākotnēji nav saistīti ar noziedzību, bet ko vāc privātie uzņēmumi, piemēram, banku, telekomunikāciju, tūrisma jomā. Plaši izmantota metode ir sociālo tīklu analīze. Prognozēšanas shēmas parasti balstās uz privātu uzņēmumu ražotu programmatūru neatkarīgi no tā, vai tie ir uzņēmumi, kas specializējas šajā jomā, vai lielie tehnoloģiju uzņēmumi.[152]

Arvien lielāku popularitāti iegūst prognozēšanas metodes, kas balstās uz sejas atpazīšanas tehnoloģijām sabiedrisko vietu uzraudzībai un analizē un vērtē cilvēku uzvedību, proti, mēģina atklāt aizdomīgu vai neparastu uzvedību. Balstoties uz datu plūsmu daudzveidību, mākslīgā intelekta sistēmas var tikt izmantotas, lai automatizētu anomāliju noteikšanu un veiktu uzvedības analīzi vai atrastu modeļus un anomālijas pamatdatos par indivīdu un iedzīvotāju uzvedību. Biometriskās identifikācijas sistēmas arvien vairāk tiek izmantotas iedzīvotāju profilēšanai, analizējot, kā cilvēki dzīvo, pārvietojas un jūtas.

Arvien biežāk tiek apgalvots, ka mākslīgā intelekta sistēmas var iemācīties interpretēt un paredzēt cilvēku rīcību, kā arī klasificēt emocijas un noteikt uzvedību kā "normālu", "nenormālu" vai "kaitīgu". Viens no argumentiem, lai veiktu šādu uzvedības analīzi, tiek minēts, ka tā var sniegt būtiskus ieguvumus, īpaši drošībai. Predikatīvās jeb paredzošās uzvedības analīzes un iedzīvotāju datu saglabāšanas (*data capturing* – angļu val.) jaunā paradigma tiek saskatīta kā risinājums humānās palīdzības, konfliktu novēršanas, miera un drošības izaicinājumiem. Tiek publicēti pētījumi, kas cenšas parādīt, ka mākslīgā intelekta un datu uztveršanas tehnoloģiju saplūšana var būtiski ietekmēt mainīgo konfliktu raksturu un pasaules drošību, tostarp saistībā ar vardarbīgu ekstrēmismu un terorismu. Tehnoloģiskā saplūšana un divējāda lietojuma sistēmu izmantošana sniedz iespējas mērķtiecīgi novērot personu un iedzīvotāju uzvedību, kā arī veikt automatizētu un prognozējošu uzvedības un situācijas analīzi, piemēram, apkopojot lielu daudzumu uzvedības un konteksta informācijas par iedzīvotājiem, kuri dzīvo nestabilās valstīs, vai par personām, kurām ir tendence uz vardarbīgu uzvedību. Tiek norādīts, ka ANO aģentūras un humānās palīdzības sniedzēji aizvien vairāk paļaujas uz digitālo platformu un privātā sektora vadošo uzņēmumu iespējām mākslīgā intelekta, prognozējošās datu analīzes un biometrisko identitātes pārvaldības sistēmu jomā, un mākslīgā intelekta un datu uztveršanas tehnoloģijas pakāpeniski ieņem arvien nozīmīgāku lomu vardarbības un konfliktu novēršanā.[153]

151 Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement.

152 Wilson (2018), Algorithmic patrol: the futures of predictive policing, p. 114.

153 Pauwels (2020), Artificial Intelligence and data capture technologies ..

Tajā pašā laikā mākslīgā intelekta un datu uztveršanas tehnoloģijas var izmantot arī prettiesiskiem mērķiem. Šīs tehnoloģijas tiek sauktas arī par divējāda lietojuma tehnoloģijām (*dual-use technologies* – angļu val.), ņemot vērā, ka tās var izmantot gan civiliem, gan militāriem mērķiem. Valstis, korporācijas, kā arī vardarbīgi nevalstiski dalībnieki tās var izmantot ļaunprātīgi, lai veiktu precīzu novērošanu.

Līdz šim nav pierādījumu, ka datu iegūšanas tehnikas, kas tiek izmantotas uzraudzībai, ir efektīvs līdzeklis, lai cīnītos pret teroristiem. Tajā pašā laikā tās ir daudz vairāk piemērotas citiem mērķiem, piemēram, sociālajai kontrolei, manipulēšanai, diskriminēšanai un pat digitālās diktatūras radīšanai.[154] Tam visspilgtākais piemērs ir Ķīna, kur mākslīgā intelekta novērošanas tehnoloģijas tiek patvaļīgi un prettiesiski izmantotas, lai kontrolētu iedzīvotājus.[155]

Ķīna ir ieviesusi un turpina attīstīt augsto tehnoloģiju novērošanas sistēmas, kas balstās uz sejas atpazīšanu un mākslīgo intelektu, lai kontrolētu tās 1,4 miljardus iedzīvotāju. Ķīnā tiek ieviesta tā sauktā "sociālā kredīta" sistēma, kas katram iedzīvotājam piešķir personisko rezultātu rādītāju. Uzraudzības sistēma ļauj kontrolēt visus iedzīvotāju personiskās dzīves aspektus, piešķirot vai atņemot punktus par pašu niecīgāko pārkāpumu. Piemēram, punkti var tikt noņemti par skaļas mūzikas klausīšanos un smēķēšanu neatļautā vietā. Ja personai ir augsts sociālais kredīts, proti, ja uzvedība ir "pareiza", tiek piešķirtas dažāda veida privilēģijas, piemēram, iespēja saņemt labus veselības aprūpes pakalpojumus, rezervēt labākās viesnīcas, nopirkt lētus lidojumus, iegūt lētus aizdevumus, tikt uzņemtam labākajās universitātēs un viegli atrast darbu. Savukārt citi, kam ir zems punktu skaits, tiek izraidīti no sabiedrības. Viņiem ir aizliegts ceļot, nav ļauts atrasties labākajās viesnīcās, saņemt kredītu, strādāt valsts iestādēs, viņi paši vai viņu bērni nevar studēt labākajās universitātēs, viņiem pat var atņemt mājdzīvnieku, kā arī publiski nosaukt par sliktu pilsoni. 2018. gadā Ķīna publicēja pilsoņu vārdus un pārkāpumus, kādus viņi izdarījuši, piemēram, kā pārkāpums tika norādīts mēģinājums caur lidostas drošības pārbaudi ienest šķiltavas. Tiesību aizstāvji ir atklājuši, ka Ķīnas valdība uzsāka uiguru novērošanu, izmantojot sejas atpazīšanu un biometrisko datu, tostarp DNS paraugu un balss paraugu, analīzi, lai prognozētu aizdomīgu uzvedību. Ķīnas varas iestādes ir izveidojušas plašu sejas atpazīšanas algoritmu sistēmu, kas ir apmācīta noteikt ādas toņus un sejas vaibstus, kas raksturīgi uiguru etniskajai piederībai. Šāda veida profilēšana padara

154 Schneier, B. (2016). *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World.* New York, London: W. W. Norton & Company, pp. 159–164.

155 Sk., piemēram, Carney, M. (17 September, 2018). Leave no dark corner. *ABC.* http://mobile.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278?pfmredir=sm&sf197878142=1&smid=Page:%20ABC%20Australia-Facebook_Organic&WT.tsrc=Facebook_Organic

Ķīnu par vadošo valsti, kas prettiesiski izmanto mākslīgo intelektu, lai uzraudzītu etniskās grupas un potenciāli varētu arī eksportēt jauna veida automatizētas rasu novērošanas tehnoloģijas.[156]

Mākslīgā intelekta novērošanas sistēmu izmantošana vismaz dažās pasaules vietās var novest pie tā, ka beidz pastāvēt sabiedrība, kuru veido brīvi autonomi pilsoņi, kuri paši izvēlas un rīkojas, pamatojoties uz brīvo gribu. Brīvā sabiedrībā pilsoņiem ir atstāta zināma rīcības brīvība starp to, kādi ir noteikumi un kas ir jāizpilda. Cilvēkiem ir atļauts "atbrīvoties" no nelieliem pārkāpumiem, tāpēc ka labi funkcionējošā sabiedrībā vairākums cilvēku lielāko daļu laika paši vēlas ievērot likumus. Uzraudzības sistēmas, kas nodrošina konkrētu likumu ievērošanu, savukārt nepieļauj izņēmumus, līdzīgi kā tos nepieļauj, piemēram, fotoradaru sistēma ceļu satiksmes pārkāpumu fiksēšanai. Arī valstīs, kurās pastāv absolūta iedzīvotāju kontrole, nekāda atkāpšanās no noteikumu neievērošanas nav pieļaujama.

Lai arī Eiropas valstīs nepastāv sociālā vērtēšanas sistēma un absolūta uz tehnoloģijām balstīta iedzīvotāju kontroles sistēma, tomēr arvien vairāk tiek izmantotas mākslīgā intelekta novērošanas tehnoloģijas, to skaitā personu vērtēšanai un uzvedības analīzei. Šī tendence ir ievērojami palielinājusies Covid-19 pandēmijas laikā.

1.2.5. Jauno novērošanas tehnoloģiju plūdi cīņā ar Covid-19

2020. gads iezīmēja strauju pagriezienu digitālo novērošanas tehnoloģiju izmantošanā. Covid-19 pandēmija radīja vēl nebijušus izaicinājumus veselības aprūpes sistēmām, kā arī dramatiskas sociālekonomiskās sekas visā pasaulē. Valstis ar lielu steigu meklēja inovatīvus veidus, kā uz datiem balstītas tehnoloģijas varētu izmantot pandēmijas ierobežošanai. Pasaule saskārās ar jaunu novērošanas tehnoloģiju plūdiem, kas tika strauji izstrādātas un ieviestas, lai labāk izprastu Covid-19 pandēmiju un cīnītos ar tās izplatību, radot jaunus izaicinājumus datu aizsardzībai un privātumam.

Esošās un jaunās digitālās tehnoloģijas tika izmantotas, lai papildinātu tradicionālos pasākumus, piemēram, sociālo distancēšanos un testēšanu, ar mērķi uzlabot to efektivitāti, lai veiktu novērošanu, tai skaitā reālā laikā, kā individuālā, tā arī sabiedrības līmenī.

Vairākas valstis salīdzinoši ātri ieviesa tehnoloģiskus risinājumus, lai palīdzētu reaģēt uz koronavīrusu un sasniegt piecus galvenos mērķus. Tie ir:

156 Wakefield, J. (26 May, 2021). AI emotion-detection software tested on Uyghurs. *BBC News.* https://www.bbc.com/news/technology-57101248; Article 19. (2021). Emotional Entanglement: China's emotion recognition market and its implications for human rights. https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf

1) karantīnas ievērošana un pārvietošanās atļaušana, lai uzzinātu, vai cilvēki atrodas tur, kur viņiem vajadzētu atrasties, vai lai atļautu pārvietoties tiem, kas nav inficēti;
2) kontaktu izsekošana, lai uzzinātu, kuri cilvēki ir bijuši saskarsmē;
3) modeļa un plūsmas modelēšana, lai noskaidrotu slimības vietu un izplatību un to, cik daudz cilvēku ir bijuši konkrētā vietā;
4) sociālās distancēšanās un pārvietošanās uzraudzība, lai zinātu, vai cilvēki ievēro ieteicamo drošo attālumu un pārvietošanās ierobežojumus;
5) simptomu izsekošana, lai zinātu, vai iedzīvotājiem ir kādi slimības simptomi.[157]

Viens no digitālajiem risinājumiem, kas tika strauji izstrādāts un ieviests, ir mobilo telefonu lietotnes. Tās tika ieviestas visā pasaulē – Ķīnā, Dienvidkorejā, Singapūrā, Izraēlā, Taivānā, Austrālijā, ASV, kā arī lielākajā daļā ES valstu. Lai gan vairākums valstu mobilās lietotnes ieviesa kontaktu fiksēšanai un izsekošanai, tomēr tās tika izveidotas arī daudziem citiem mērķiem: lai sniegtu informāciju; lai sniegtu jaunākās ziņas, brīdinātu un sniegtu instrukcijas iedzīvotājiem; lai sniegtu medicīnisko atbalstu; lai iedzīvotāji varētu paši diagnosticēt vai ziņot par saslimšanu; sabiedrības kontrolei, t. i., gan brīvprātīgas, gan piespiedu lietotnes karantīnas ievērošanas kontrolei un pārvietošanās kontrolei; lai informētu par pārkāpumiem.[158]

Ieviest tehnoloģiju risinājumus cīņā ar pandēmiju mudināja daudzas starptautiskas organizācijas. Divas dienas pēc Covid-19 pasludināšanas par pandēmiju, 2020. gada 13. martā, Pasaules Veselības organizācija aicināja valstis kopā ar testēšanu, sociālo distancēšanos un citiem pasākumiem izsekot kontaktus, lai novērstu infekcijas un glābtu dzīvības.[159]

Anonimizētu mobilitātes datu izmantošana un kontaktu izsekošana, izmantojot mobilās lietotnes, bija pirmā ES valstu kopīgā un koordinētā atbildes reakcija uz Covid-19 pandēmiju. 2020. gada 8. aprīlī Eiropas Komisija pieņēma ieteikumu, lai izstrādātu kopīgu pieeju, sauktu par rīkkopu, lai krīzes pārvarēšanā izmantotu digitālus līdzekļus, it īpaši mobilās lietotnes un anonimizētus datus par

157 Countries are using apps and data networks to keep tabs on the pandemic. (26 March, 2020). *The Economist.* https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic; sk. arī Whitelaw, S., Mamas, A., Topol, E., van Spall, H. G. C. (2020). Applications of Digital Technology in COVID-19 Pandemic Planning and Response. *The Lancet Digital Health,* 2(8). https://doi.org/10.1016/S2589-7500(20)30142-4.

158 Council of Europe. (2020). Digital Solutions to fight COVID-19. 2020 Data Protection Report. https://rm.coe.int/report-dp-2020-en/16809fe49c

159 WHO. (13 March, 2020). WHO Director-General's opening remarks at the media briefing on COVID-19 – 13 March 2020. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing--14-september-2022

iedzīvotāju mobilitāti.[160] 2020. gada 15. aprīlī Eiropadome un Eiropas Komisija pieņēma kopīgo Eiropas ceļvedi, uzsverot, ka ES veic pasākumus, lai atbalstītu kontaktu izsekošanas lietotnes, kā arī apkopotu un anonimizētu datu apstrādi no sociālo mediju un mobilo tīklu operatoriem kā papildu pasākumus, kas palīdzētu atcelt pulcēšanās, ceļošanas un cita veida ierobežojumus.[161] Dokumentos norādīts, ka anonimizētu atrašanās vietu un kustības datu apstrāde no mobilajiem telefoniem un sociālo mediju lietotnēm var palīdzēt cīņā ar pandēmiju, jo šāda apstrāde var atklāt sociālās mobilitātes modeļus un tendences un var izrādīties noderīga vīrusa izplatības prognozēm.

Plašas diskusijas izraisīja kontaktu izsekošanas lietotnes. Visu šo lietotņu mērķis ir retrospektīvi izsekot un brīdināt apstiprināto inficēto personu kontaktpersonas. Tomēr valstis izvēlējās dažādas pieejas, kā ieviest šīs lietotnes, un dažas valstis, piemēram, Norvēģija[162] un Lietuva[163], kas pirmās steidzās tās ieviest, vēlāk bija spiestas tās apturēt privātuma pārkāpumu dēļ.

2021. gada 17. martā Eiropas Komisija publicēja priekšlikumu regulai par digitālā zaļā sertifikāta ieviešanu, lai atvieglotu brīvu pārvietošanos Covid-19 pandēmijas laikā.[164] Ideja par vakcinācijas sertifikātu ieviešanu ātri tika īstenota daudzās Eiropas un pasaules valstīs, vienlaikus izraisot plašas diskusijas, it īpaši par to atbilstību vienlīdzības un nediskriminācijas principiem.[165] Dānija kļuva par pirmo Eiropas valsti, kas 2021. gada aprīlī ieviesa vakcīnas sertifikātus un

160 Komisijas Ieteikums (ES) 2020/518 (2020. gada 8. aprīlis) par vienotu Savienības rīkkopu tehnoloģiju un datu izmantošanai ar mērķi apkarot Covid-19 krīzi un iziet no tās, it īpaši attiecībā uz mobilajām lietotnēm un anonimizētu mobilitātes datu izmantošanu. *OV L* 114/7, 14.04.2020.

161 Eiropadome un Eiropas Komisija. (2020). Kopīgais Eiropas ceļvedis Covid-19 ierobežošanas pasākumu atcelšanai. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020XC0417(06)&from=EN

162 Manancourt, V. (15 June, 2020). Norway suspends contact-tracing app over privacy concerns. *POLITICO.* https://www.politico.eu/article/norway-suspends-contact-tracing-app-over-privacy-concerns/

163 Pugh, A. (28 May, 2020). Lithuanian contact tracing app suspended. *Global Data Review.* https://globaldatareview.com/coronavirus/lithuanian-contact-tracing-app-suspended

164 Eiropas Komisija. (2021). Priekšlikums. Eiropas Parlamenta un Padomes regula par sadarbspējīgu vakcinācijas, testēšanas un pārslimošanas sertifikātu izdošanas, verifikācijas un akceptēšanas satvaru nolūkā atvieglot brīvu pārvietošanos Covid-19 pandēmijas laikā (digitālais zaļais sertifikāts). https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52021PC0130&from=EN

165 Sk., piemēram, EDPB, EDPS. (2021). EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate). https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042021-proposal_en

izmantoja tos restorānos, bāros, pat universitātēs. Latvijā digitālie Covid-19 sertifikāti tika ieviesti 2021. gada jūnijā un izmantoti, lai varētu apmeklēt izklaides un sporta pasākumus, piemēram, pasaules hokeja čempionāta spēles, teātrus, koncertus, kafejnīcas iekštelpās, bet vēlāk arī lai ierobežotu nevakcinēto personu iespējas mācīties un strādāt. Šāda digitālo sertifikātu izmantošana radīja daudzus jautājumus par to samērīgumu un atbilstību cilvēktiesībām, un tie nonāca arī līdz tiesai.[166]

Valstis izmantoja arī cita veida tehnoloģijas, lai ierobežotu pandēmijas izplatību, to skaitā mobilās un biometriskās lietotnes, elektroniskās aproces un citas biometriskās valkājamās ierīces, termālās kameras, kā arī attālinātu novērošanu ar droniem un robotiem.[167] Tālāk sniegti daži piemēri, lai parādītu uzraudzības tehnoloģiju ieviešanu dažādās pasaules valstīs.

Ķīnā valsts iestādes iedzīvotājiem uzlika pienākumu augšupielādēt mobilo lietotni un skenēt kvadrātkodu pie ieejas institūcijās, lai pārbaudītu personas infekcijas statusu un atļautu tai iekļūt iepirkšanās centros, metro un citās sabiedriskās vietās, un šī lietotne nosūta brīdinājumu vietējai policijai, ja personai ir jāatrodas karantīnā un tā nedrīkst atrasties ārpus dzīvesvietas.[168]

Līdzīgi Krievijā, Maskavā, valsts iestādes ieviesa lietotņu sistēmu, lai iedzīvotājiem apstiprinātu braucienus pa izvēlēto maršrutu un ieviestu karantīnu. Reģistrējoties sistēmā, personai vajadzēja sasaistīt savu mobilo telefonu ar pilsētas e-pārvaldes sistēmu un augšuplādēt personas apliecību, informāciju par darba devēju un transportlīdzekļa numura zīmi.[169] Krievijā un Moldovā, lai kontrolētu karantīnas ievērošanu, tika izmantotas arī sejas atpazīšanas tehnoloģijas.[170]

Taivānā tika ieviesta obligāta tālruņa atrašanās vietas izsekošanas sistēma, lai nodrošinātu karantīnu. Iedzīvotājiem, kuriem nebija savu telefonu, tika izsniegti

166 Sk., piemēram, Satversmes tiesas 2022. gada 18. februāra lēmums lietā Nr.2021-10-03.

167 Sk., piemēram, Vargo, D., et al. (2021). Digital Technology Use during COVID-19 Pandemic: A Rapid Review. *Human Behavior and Emerging Technologies,* 3(1), pp. 13–24. https://doi.org/10.1002/hbe2.242; Kitchin, R. (2020). Civil Liberties or Public Health, or Civil Liberties and Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19. *Space and Polity*, 24(3), pp. 362–381. https://doi.org/10.1080/13562576.2020.1770587; Couch, Robinson, Komesaroff (2020), COVID-19 – Extending Surveillance ..

168 Goh, B. (26 February, 2020). China rolls out fresh data collection campaign to combat coronavirus. *Reuters.* https://www.reuters.com/article/us-china-health-data-collection/china-rolls-out-fresh-data-collection-campaign-to-combat-coronavirus-idUSKCN20K0LW

169 Ilyushina, M. (14 April, 2020). Moscow rolls out digital tracking to enforce lockdown. Critics dub it a 'cyber Gulag'. *CNN*. https://edition.cnn.com/2020/04/14/world/moscow-cyber-tracking-qr-code-intl/index.html

170 Ball, S. (24 March, 2020). 100,000 cameras: Moscow uses facial recognition to enforce quarantine. *France24.* https://www.france24.com/en/20200324-100-000-cameras-moscow-uses-facial-recognition-to-enforce-quarantine

telefoni, kuros aktivizēta atrašanās vietas noteikšana ar GPS. Ja persona izgāja ārpus noteiktajai robežai, kurā tai jāatrodas atbilstoši pārvietošanās ierobežojumiem, viņai tika nosūtīta īsziņa un uzlikts naudas sods par pārkāpumu.[171] Kāds ASV universitātes students, kurš atradās Taivānā karantīnā, tika aizvests uz policijas iecirkni pēc tam, kad viņa telefona akumulators bija izlādējies, kamēr viņš naktī gulēja.[172]

Lai nodrošinātu obligātās mājas karantīnas ievērošanu, Honkonga ieviesa elektroniskās izsekošanas aproces.[173] Izraēlā digitālās novērošanas rīki, kurus parasti lieto pretterorisma nolūkā, tika izmantoti, lai izsekotu personas, kurām apstiprināta saslimšana ar koronavīrusu, respektīvi, noteiktu šo personu telefonu atrašanās vietu 14 dienu laikā pirms pozitīvās pārbaudes, lai noskaidrotu kontaktpersonas.[174]

Dienvidkorejā valdība izmantoja novērošanas kameru ierakstus, viedtālruņu atrašanās vietas datus un kredītkaršu ierakstus par pirkumiem, lai izsekotu pozitīvus vīrusa testu gadījumus un to kontaktus.[175]

Austrālijā[176] un ASV[177] tika ieviestas potīšu aproces, nosakot pienākumu tās uzlikt personām, kuras neievēro karantīnas vai pašizolācijas prasības.

Arī Eiropas valstīs, lai cīnītos ar pandēmiju, tika ieviestas dažādas jaunas tehnoloģijas un risinājumi, kuru izmantošanu pirms pandēmijas būtu grūti iedomāties. Piemēram, Itālija, Grieķija, Beļģija un Ungārija izmantoja dronus vai robotus, lai uzraudzītu fiziskās distancēšanās ievērošanu sabiedriskās vietās. Grieķijā un Itālijā, kā arī Vācijā Diseldorfā un Dortmundē valsts iestādes izmantoja dronus,

171 Timberg, C., Harwell, D. (19 March 2020). Government efforts to track virus through phone location data complicated by privacy concerns. *The Washington Post.* https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/

172 Stanley, J., Granick, J. S. (2020). The Limits of Location Tracking in an Epidemic. ACLU. https://www.aclu.org/wp-content/uploads/legal-documents/limits_of_location_tracking_in_an_epidemic.pdf

173 Ibid.

174 Halbfinger, D. M., Kershner, I., Bergman, R. (18 March, 2020). To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data. *The New York Times.* https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html

175 Hendry, J. (19 April, 2020). WA to electronically track COVID-19 patients who defy isolation orders. *iTnews*. https://www.itnews.com.au/news/wa-to-electronically-track-covid-19-patients-who-defy-isolation-orders-546224

176 Singer, N., Sang-Hun, C. (23 Mach, 2020). As Coronavirus Surveillance Escalates, Personal Privacy Plummets. *The New York Times*. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

177 Kallingal, M. (3 April, 2020). Ankle monitors ordered for Louisville, Kentucky residents exposed to Covid-19 who refuse to stay home. *CNN*. https://edition.cnn.com/2020/04/03/us/kentucky-coronavirus-residents-ankle-monitors-trnd/index.html

lai liktu gājējiem doties mājās un atstāt sabiedriskās vietas. Savukārt Horvātijā droni tika izmantoti, arī lai mērītu cilvēku temperatūru.[178]

Slovēnija pieņēma likumu, kas paredz, ka policija drīkst izmantot dažādas metodes, lai nodrošinātu, ka pilsoņi ievēro karantīnu un citus ierobežojošos pasākumus, un kas atļauj izmantot sejas atpazīšanu, lai apturētu un identificētu personas.[179]

Vācija ieviesa viedpulksteņa lietotni, kas vāc datus par pulsu, temperatūru un miegu, lai pārbaudītu vīrusa izraisītās slimības pazīmes. Lietotnes dati tika rādīti tiešsaistē, interaktīvā kartē, kurā iestādes var novērtēt Covid-19 sastopamības varbūtību visā valstī.[180]

Lihtenšteina, Kipra un Francija izstrādāja un ieviesa elektroniskās aproces. Lihtenšteina testēja elektronisko aproci, kas mēra ādas temperatūru, pulsu, elpošanu, asinsspiedienu. Vairāk nekā 2000 iedzīvotāju to testēja, lai noskaidrotu, vai tā var palīdzēt atklāt Covid-19 infekciju agrīnā fāzē.[181]

Savukārt Beļģijā Antverpenes ostā tika ieviestas aproces, kas izmanto *Bluetooth* tehnoloģiju, lai kontrolētu sociālās distancēšanās prasību izmantošanu darba vietā. Aproce signalizē, ja strādnieki atrodas pārāk tuvu cits citam. Turklāt Beļģijas datu aizsardzības iestāde apstiprināja, ka šādas aproces var tikt izmantotas ar nosacījumu, ka personu atrašanās vietas dati netiek vākti un glabāti, kā arī ja ir saņemta īpaša piekrišana. Brīva piekrišana gan ir visai apstrīdama, ņemot vērā, ka darba devējs un darbinieks neatrodas līdztiesīgās pozīcijās.[182]

Lai gan biometriskās valkājamās ierīces nevienā no ES valstīm nebija obligātas, tajā pašā laikā daudzie eksperimenti ar tām radīja bažas, ka turpmāk arvien biežāk varētu tikt ieviestas šāda veida ierīces un citas tehnoloģijas, kas vāc biometriskos datus un izmanto tos dažādiem mērķiem. Spilgts piemērs šādai attīstības tendencei ir Singapūra, no kuras daudzas valstis ņēma piemēru, ieviešot kontaktu izsekošanas lietotnes. Singapūra viena no pirmajām ātri ieviesa lietotni "TraceTogether", kas izmanto *Bluetooth* tehnoloģiju, nosaka un uzglabā informāciju par tuvumā esošiem telefoniem un ļauj izsekot kontaktus.[183] Lai gan

178 FRA. (2020). Coronavirus pandemic in the EU – Fundamental Rights Implications – Bulletin 2. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf

179 Kučić, L. J. (7 July, 2020). Slovenian police acquires automated tools first, legalizes them later. *Algorithm Watch*. https://algorithmwatch.org/en/slovenia-police-face-recognition/

180 Busvine, D. (7 April, 2020). Germany launches smartwatch app to monitor coronavirus spread. *Reuters.* https://www.reuters.com/article/us-health-coronavirus-germany-tech-idUSKBN21P1SS

181 Council of Europe (2020), Digital solutions to fight COVID-19.

182 Ibid.

183 Singer, Sang-Hun (23 Mach, 2020), As Coronavirus Surveillance Escalates, Personal Privacy Plummets.

lietotni lejuplādēja ceturtdaļa iedzīvotāju, t. i., 1,5 no 5,7 miljoniem, izrādījās, ka šis skaits bija pārāk mazs, lai tā varētu efektīvi palīdzēt cīnīties ar pandēmiju, savukārt obligāta tās lietošana netika noteikta, jo tā nedarbojās visās "Apple" *iOS* iekārtās. Tāpēc Singapūra nolēma izstrādāt jaunu tehnoloģiju – Covid-19 kontaktu izsekošanas valkājamo ierīci, kuru varētu izdalīt ikvienam valsts iedzīvotājam. 2020. gada septembrī Singapūra sāka šo valkājamo ierīču izdalīšanu valsts iedzīvotājiem, nosakot obligātu to lietošanu ceļotājiem, lai uzraudzītu karantīnas ievērošanu.[184]

Minētie piemēri spilgti parāda, cik ātri valstis var ieviest jaunas digitālās tehnoloģijas un risinājumus, kas ierobežo personu tiesības un brīvības. Šīs jaunās tehnoloģijas ir radījušas plašas diskusijas par to atbilstību cilvēktiesībām, īpaši tiesībām uz privātumu un datu aizsardzību, un jautājumus par to, cik lielā mērā cilvēktiesības var tikt ierobežotas ārkārtas situācijā.

Digitālo tehnoloģiju, tostarp lielo datu un mākslīgā intelekta, izmantošana vīrusa izplatības ierobežošanai un kontaktu izsekošanai rada bažas ne tikai par to ietekmi uz pamattiesībām, bet arī par šo tehnoloģiju turpmāku izmantošanu masveida novērošanas nolūkā pēc krīzes. Vēsturnieks Juvāls Noa Harari brīdina, ka mēs esam liecinieki jaunu uzraudzības sistēmu radīšanai visā pasaulē, ko veic gan valsts, gan privātie uzņēmumi. Krīze var iezīmēt nozīmīgu pavērsienu novērošanas tehnoloģiju izmantošanā, jo tā var normalizēt masveida novērošanas pasākumu izmantošanu valstīs, kuras līdz šim tos ir noraidījušas.[185] Stingra jauno tehnoloģiju izmantošanas pārraudzīšana gan pandēmijas laikā, gan pēc tās ir nepieciešama, ne tikai lai aizsargātu cilvēktiesības, bet arī lai masveida novērošanas pasākumi nekļūtu par jauno normu.

184 Mohan, M. (12 September, 2020). More than 3,500 electronic wristband devices issued to travellers serving stay-home notices: ICA. *CNA.* https://www.channelnewsasia.com/news/singapore/electronic-wristband-devices-stay-home-notice-ica-covid-19-13105390

185 Harari (2020), Yuval Noah Harari: "Every crisis is also an opportunity."

2. DAĻA

Mākslīgā intelekta novērošanas pasākumu ietekme uz cilvēktiesībām

Cilvēktiesības, demokrātija un tiesiskums ir Eiropas valstu pamatvērtības. Mākslīgais intelekts rada būtiskus izaicinājumus šīm vērtībām. Mākslīgā intelekta novērošanas pasākumi apdraud privātumu, datu aizsardzību un arī citas cilvēktiesības, uz ko lielu uzmanību ir vērsusi Eiropas Padome[186] un ES[187], kā arī citas starptautiskās organizācijas. Šie pasākumi var radīt arī plašāku negatīvu ietekmi uz demokrātiju un tiesiskumu, ko var būt grūti paredzēt un izmērīt.

Laika gaitā ir izstrādātas starptautiskas cilvēktiesību normas un to aizsardzības mehānismi, kas nosaka to, kādā veidā ir jāizturas pret ikvienu personu. ANO 1948. gada Vispārējā cilvēktiesību deklarācija[188], iespējams, ir nozīmīgākais starptautiskais cilvēktiesību dokuments, kura pamatā ir apņemšanās, ka tas, kas notika Otrā pasaules kara laikā, ir ne tikai jānosoda un jāaizliedz, bet to nekad nedrīkst atkārtot. 1966. gadā ANO pieņēma Starptautisko paktu par pilsoniskajām un politiskajām tiesībām (SPPPT)[189], kas Latvijā ir spēkā no 1992. gada 14. jūlija. Līdzās globālajām tiesību sistēmām, kāda ir ANO, cilvēktiesības ir aizsargātas arī reģionālā un nacionālā līmenī.

1949. gadā izveidotā Eiropas Padome ir izstrādājusi vienotus cilvēktiesību aizsardzības standartus, kā arī radījusi efektīvu to aizsardzības mehānismu. Viens no būtiskākajiem starptautiskajiem cilvēktiesību dokumentiem ir 1950. gada 4. novembrī Eiropas Padomes pieņemtā ECTK, kura Latvijā ir spēkā no 1997. gada. Lai nodrošinātu, ka dalībvalstis ievēro tajā noteiktās cilvēktiesības, tika izveidota ECT, kuras kompetencē ir izskatīt iedzīvotāju sūdzības un piemērot soda sankcijas

186 Sk., piemēram, Eiropas Padomes Ministru komitejas Rekomendāciju CM/Rec(2020)1 dalībvalstīm par algoritmisko sistēmu ietekmi uz cilvēktiesībām, kas pieņemta 08.04.2020.: Council of Europe (2020), Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States ..

187 Eiropas Komisija (2020), Baltā grāmata par mākslīgo intelektu; European Parliament. (2020). Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies. https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html; Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.
Vairāk par ES mākslīgā intelekta regulējumu skat. grāmatas 4.2.5. nodaļā.

188 Vispārējā cilvēktiesību deklarācija. Pieņemta 10.12.1948. (Latvijā spēkā no 22.05.1990.). https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/lat.pdf

189 Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām. Pieņemts 16.12.1966. (Latvijā spēkā no 14.07.1992.). *Latvijas Vēstnesis*, 23.04.2003., Nr. 61.

pret valsti, kas pārkāpusi viņu tiesības. Valstīm, kurām ir saistoša ECTK, ir jāievēro tajā noteiktās tiesības, kā arī ECT sniegtās atziņas par minēto tiesību interpretāciju.

Cilvēktiesību aizsardzība ieņem primāru nozīmi arī ES. Lai gan sākotnēji ES tika veidota kā ekonomiska kopiena, pakāpeniski paplašinoties tās funkcijām, arvien vairāk tika atzīta cilvēktiesību būtiskā nozīme. Līgumā par Eiropas Savienību (LES) pamattiesību ievērošanas princips ir atzīts par ES vispārējo tiesību principu, kā arī noteikts, ka ES respektē pamattiesības atbilstoši ECTK un dalībvalstu kopīgām konstitucionālām tradīcijām.[190] Būtisks solis cilvēktiesību aizsardzībā ir Hartas pieņemšana 2000. gadā. Tajā iekļautas visas ECTK noteiktās tiesības, kā arī citas tiesības un principi, kuri izriet no ES dalībvalstu kopējām konstitucionālajām tradīcijām, EST judikatūras un citiem starptautiskiem instrumentiem. Harta ir moderns tiesību akts un ietver "trešās paaudzes" pamattiesības, tostarp tiesības uz datu aizsardzību. Līdz ar Lisabonas līguma spēkā stāšanos 2009. gadā Harta kļuva par juridiski saistošu dokumentu ES iestādēm un dalībvalstīm. Izstrādājot ikvienu jaunu ES tiesību aktu, ir jāizvērtē tā ietekme un atbilstība Hartā noteiktajām pamattiesībām. ES valstīm ir pienākums ievērot Hartu, īstenojot ES tiesību aktus, ko uzrauga Eiropas Komisija, kā arī EST. Harta papildina arī valstu sistēmas, bet tās neaizstāj. Cilvēktiesības tiek nacionāli aizsargātas valstu konstitūcijās. Latvijas Republikas Satversmes (Satversme) atsevišķa nodaļa ir veltīta cilvēka pamattiesībām.

Nodaļas turpinājumā aplūkotas cilvēktiesības, kuras mākslīgā intelekta novērošanas pasākumi ietekmē visvairāk, t. i., cilvēka cieņa, privātums un datu aizsardzība, diskriminācijas aizliegums, tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu, izteiksmes brīvība, pulcēšanās un biedrošanās brīvība. Nodaļā turklāt atklāts, kā mākslīgā intelekta novērošanas pasākumi līdzās cilvēktiesību apdraudējumam var radīt arī plašāku apdraudējumu demokrātiskām vērtībām. Nodaļas nobeigumā vērsta uzmanība uz to, ka krīzes situācijās, kad valstis strauji cenšas ieviest dažādus drošības pasākumus, pienākums ievērot cilvēktiesības netiek atcelts.

2.1. Cilvēka cieņa

Cilvēka cieņas jēdziens ietver uzskatu, ka ikvienam no mums ir "iekšēja vērtība", ko nekad nedrīkst mazināt, nedrīkst apdraudēt vai apspiest citas personas, arī izmantojot mākslīgo intelektu vai citas tehnoloģijas.[191] Eiropas Datu aizsardzības

190 Līgums par Eiropas Savienību (konsolidētā versija), OV C 115/13, 09.05.2008.

191 McCrudden, C. (2008). Human Dignity and Judicial Interpretation of Human Rights. *European Journal of International Law*, 19(4), pp. 655–724. https://doi.org/10.1093/ejil/chn043

uzraudzītājs ir norādījis, ka cilvēka cieņas garantēšana varētu būt pretsvars visaptverošai novērošanai un varas asimetrijai, ar ko šobrīd saskaras indivīds. Tai ir jābūt jaunās digitālās ētikas centrā.[192]

Cilvēka cieņa ir ne tikai pamattiesība pati par sevi, bet arī visu pārējo tiesību pamats. ANO Vispārējās cilvēktiesību deklarācijas 1. pants nosaka, ka visi cilvēki piedzimst brīvi un vienlīdzīgi cieņā un tiesībās. Satversmes tiesa ir atzinusi, ka cilvēka cieņa un katra indivīda vērtība ir pamattiesību būtība.[193] No Latvijas kā neatkarīgas, demokrātiskas un tiesiskas valsts pamatnormas izriet, ka cilvēka cieņa ir valsts konstitucionāla vērtība. Cilvēka cieņa raksturo cilvēku kā augstāko demokrātiskas tiesiskas valsts vērtību. Katra indivīda vērtība ir pamattiesību būtība.[194] Tiesību zinātniece profesore Sanita Osipova norāda: "Cilvēka cieņa ir iemesls, kāpēc jāpastāv demokrātiskai tiesiskai valstij. Cieņa ir cilvēka vērtība un tiesības uz pašnoteikšanos, tā ietver brīvību un atbildību par saviem lēmumiem."[195]

Cilvēka cieņa ir gan Satversmes, gan ES tiesību pamatā. Satversmes ievadā ir norādīts, ka Latvija kā demokrātiska un tiesiska valsts balstās uz cilvēka cieņu un brīvību. Kā pamattiesība tā ir noteikta Satversmes 95. pantā, kas paredz, ka valsts aizsargā cilvēka godu un cieņu. Cilvēka cieņa kā absolūta pamattiesība ir atzīta arī ES. Tā ir noteikta LES 2. pantā un Hartas 1. pantā, kas nosaka: "Cilvēka cieņa ir neaizskarama. Tā ir jāaizsargā un jārespektē."

Cilvēka cieņa vispirms ir jāaizsargā attiecībās starp valsti un cilvēku. Vislabāk šo nepieciešamību ir izskaidrojusi S. Osipova. Viņa norāda, ka konstitucionālisms, demokrātija un tiesiska valsts, t. i., valsts, kuru mēs atzīstam par saderīgu ar mūsdienu pasauli, tika veidotas, pamatojoties uz liberālām vērtībām. Tomēr šīs radikālās izmaiņas tika panāktas tikai tāpēc, ka to prasīja jaunais uzskats – cilvēks ir saprātīgs un viņam ir tiesības uz pašnoteikšanos. Cilvēks ir vērtība, kam piešķirta neatņemama cieņa un kas ir juridiski jāaizsargā no valsts patvaļas. Tendence atbrīvot sabiedrību no iespējamiem draudiem, ierobežojot cilvēka izvēles brīvību un tiesības, spilgti izpaudās, attīstoties zinātnei, pirmkārt,

192 EDPS. (2015). Opinion 4/2015 Towards a New Digital Ethics Data, Dignity and Technology. https://edps.europa.eu/sites/default/files/publication/15-09-11_data_ethics_en.pdf

193 Satversmes tiesa ir atzinusi, ka cilvēka cieņa un katra indivīda vērtība ir pamattiesību būtība. Satversmes tiesas 2019. gada 5. marta spriedums lietā Nr. 2018-08-03; sk. arī Waldron, J. (2013). Is Dignity the Foundation of Human Rights? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2196074

194 Sk., piemēram, Satversmes tiesas 2020. gada 20. novembra spriedumu lietā 2019-33-01, 12.2. punktu un tajā citēto judikatūru.

195 Satversmes tiesa. (2020. gada 2. decembris). Satversmes tiesas priekšsēdētāja Sanita Osipova akcentē cilvēka cieņas un iecietības nozīmi pamattiesību īstenošanā. *Jurista Vārds.* https://juristavards.lv/zinas/277771-satversmes-tiesas-priekssedetaja-sanita-osipova-akcente-cilveka-cienas-un-iecietibas-nozimi-pamattiesibu-istenosana/

dabaszinātnēm. Zinātne identificēja "potenciālos draudus" sabiedrības nākotnes labklājībai, savukārt valsts ar likumiem un to piemērošanu preventīvi novērsa šos "potenciālos draudus". 20. gadsimtā mēģinājumi izmantot visjaunākos zinātniskos atklājumus sabiedrības atdzīvināšanai tika veikti daudzās valstīs, pirmkārt, identificējot "nelabvēlīgas personas" un pēc tam ierobežojot viņu tiesības un tās iznīcinot. Visiem plaši ir zināmas nacistiskajā Vācijā veiktās represijas pret noteiktu sabiedrības daļu, īpaši ebrejiem, vai komunistiskajā PSRS – pret "tautas ienaidniekiem". Tikai tiesiskas valsts un pamattiesību konsolidācija pielika punktu šausminošajiem sociālajiem eksperimentiem, kas nesamērīgi ierobežoja dažu cilvēku tiesības uz pašnoteikšanos vienā no vissvarīgākajām jomām – pašnoteikšanās pār savu ķermeni.[196]

Mūsdienās 21. gadsimtā biotehnoloģiju un informācijas tehnoloģiju straujā attīstība un apvienošanās ir radījusi daudzus jaunus jautājumus par ētiskajām un tiesiskajām robežām, līdz kādām ir pieļaujams eksperimentēt ar cilvēka ķermeni un prātu. Kā norāda ASV tiesību zinātniece Džūlija Koena (*Julie E. Cohen*), skats uz cilvēka dabu, ko pastiprina datu apstrādes algoritmi, ir gan nepiedodams, gan arī nežēlīgs.[197] Jauno tehnoloģiju, īpaši mākslīgā intelekta, attīstība, tai skaitā biometriskie masveida novērošanas pasākumi, liek no jauna pārvērtēt un noteikt skaidras sarkanās līnijas šo tehnoloģiju izmantošanai. Vislabākais veids, kā to izdarīt, ir izvērtēt šo tehnoloģiju ietekmi uz cilvēktiesībām, lai gan noteikt, kādos gadījumos tās tiek pārkāptas un nesamērīgi ierobežotas, arī nepavisam nav vienkāršs uzdevums.

Cilvēka cieņa ir būtisks elements Eiropas pieejai attiecībā uz datu apstrādi un aizsardzību. Cilvēka cieņa ir bieži ietverta nesaistošos instrumentos, kas regulē mākslīgo intelektu.[198] No cilvēka cieņas principa izriet arī cilvēka pārākuma princips, kas nozīmē arī cilvēka prioritāti pār zinātni. Atzīstot cilvēka pārākumu mākslīgā intelekta kontekstā, mākslīgā intelekta sistēmām jābūt izveidotām tā, lai tās kalpotu cilvēcei, un šo sistēmu izveidē, attīstībā un izmantošanā pilnībā jāievēro cilvēktiesības, demokrātija un tiesiskums.[199]

196 Osipova (2020), Bioethics in Correlation with the Principle of Human Dignity, pp. 121–136.

197 Cohen, J. E. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Stan. L. Rev.*, 52, pp. 1373–1438.

198 UNESCO (2021), Recommendation on the Ethics of Artificial Intelligence, point 13; OECD (2019), Recommendation of the Council on Artificial Intelligence.

199 Mantelero, A. (2020). Regulating AI within the Human Rights Framework: A Roadmapping Methodology, p. 487. In: Czech, P., Hesch, L., Lukas, K., Nowak, M., Oberleitner, G. (eds.), *European Yearbook on Human Rights.* Interesentia, pp. 477–502.

2.2. Privātums un datu aizsardzība

Mākslīgā intelekta novērošanas tehnoloģiju ieviešana un izmantošana būtiski ierobežo gan tiesības uz privāto dzīvi, gan tiesības uz personas datu aizsardzību, kas ietver arī ES datu aizsardzības regulējumu.

Tiesības uz privātumu ir starptautiski atzītas cilvēka pamattiesības, kas atrodamas galvenajos cilvēktiesību dokumentos. Tiesības uz privāto dzīvi jeb tiesības uz privātumu ir noteiktas Vispārējās cilvēktiesību deklarācijas 12. pantā, ECTK 8. pantā un Hartas 7. pantā. Tiesības uz datu aizsardzību kā patstāvīgas pamattiesības ir ietvertas Hartas 8. pantā. Lai gan šīs abas tiesības ir cieši saistītas, tās ir atšķirīgas un patstāvīgas tiesības un tiek apzīmētas arī kā "klasiskās" tiesības uz privātās dzīves aizsardzību un "modernās" tiesības uz datu aizsardzību.[200] It īpaši Eiropā šo tiesību aizsardzība tiek uzskatīta par demokrātiskas un tiesiskas valsts būtisku elementu. ES ir noteikti augsti privātuma un datu aizsardzības standarti, kas būtiski ietekmē datu aizsardzības tiesību attīstību visā pasaulē.

Tiesības uz privātās dzīves neaizskaramību noteiktas arī Satversmes 96. pantā. Satversmes tiesas praksē ir nostiprinājusies atziņa, ka Satversmes šajā pantā noteiktās tiesības uz privātās dzīves neaizskaramību ietver fiziskās personas datu aizsardzību. Konkretizējot Satversmes 96. pantā ietvertās tiesības, Satversmes tiesa ir norādījusi, ka tās aizsargā indivīda fizisko un garīgo integritāti, godu un cieņu, vārdu un identitāti, personas datus.[201]

Tiesībām uz privāto dzīvi un datu aizsardzību ir primāra nozīme, izvērtējot mākslīgā intelekta novērošanas tehnoloģijas. Grāmatas nākamajā nodaļā detalizēti analizēts, kā šīs abas pamattiesības ir piemērojamas, nosakot aizsardzības garantijas un robežas šo tehnoloģiju izmantošanai. Tāpat atklāts, kā šīs abas tiesības tiecas aizsargāt arī citas pamatvērtības, kā cilvēka cieņa un autonomija, piešķirot mums personisko sfēru, kurā varam brīvi attīstīt savu personību, domāt un veidot savu viedokli. Šīs tiesības ir būtisks priekšnoteikums arī citu cilvēktiesību īstenošanai, kuras apdraud masveida novērošanas pasākumi, piemēram, vārda un informācijas brīvības un pulcēšanās un biedrošanās brīvības īstenošanai.

Jebkura veida novērošana ir iejaukšanās tiesībās uz privātumu un tiesībās uz personas datu aizsardzību. Jau 2010. gadā profesore Helena Nisenbauma (*Helen*

200 ES Pamattiesību aģentūra, ECT, EP, EDAU (2018), Rokasgrāmata – Eiropas Savienības Pamattiesību aģentūra, Eiropas Cilvēktiesību tiesa, Eiropas Padome, Eiropas Datu aizsardzības uzraudzītājs. (2018). Rokasgrāmata par Eiropas tiesību aktiem datu aizsardzības jomā. 2018. gada izdevums. http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law

201 Sk., piemēram, Satversmes tiesas 2019. gada 6. marta spriedumu lietā Nr. 2018-11-01, 16.1. punktu; Satversmes tiesas 2016. gada 16. marta spriedumu lietā Nr. 2015-14-0103, 15.1. punktu un tajos norādītos spriedumus.

Nissenbaum) vērsa uzmanību, ka informācijas tehnoloģijas tiek uzskatītas par lieliem draudiem privātumam, jo tās ļauj visaptveroši novērot, izveidot masveida datubāzes un zibens ātrumā izplatīt informāciju visā pasaulē.[202] Ir pašsaprotami, ka mūsu privātumu apdraud nepārtrauktie tehnoloģiskie sasniegumi pēdējās desmitgadēs, tie ir padarījuši novērošanas, izsekošanas un profilēšanas paņēmienus vieglākus, lētākus un precīzākus, kā rezultātā novērošana ir ievērojami palielinājusies gan publiskajā, gan privātajā sektorā. Vēl vairāk to veicina mākslīgā intelekta un biometrisko tehnoloģiju attīstība.

Sejas atpazīšanas tehnoloģiju izmantošana ietver biometrisko datu – sejas attēlu – iegūšanu, salīdzināšanu un uzglabāšanu informācijas sistēmās identifikācijas nolūkos. Katra no šīm darbībām ir uzskatāma par iejaukšanos tiesībās uz privāto dzīvi un tiesībās uz personas datu aizsardzību. Sejas attēls ir personas dati, ko apstiprina arī EST[203] un ECT[204]. ECT ir arī atzinusi, ka sejas attēls ir viens no galvenajiem cilvēka personības atribūtiem, jo tas atklāj personas unikālās īpašības un atšķir mūs citu no cita. Tādējādi tiesības uz sejas attēla aizsardzību ir viena no būtiskākajām personības attīstības sastāvdaļām.[205]

ECTK 8. pantā ir ietverts plašs mūsu privātās dzīves aizsardzības elementu klāsts, ko var iedalīt trīs lielās kategorijās, proti:

1) personas (vispārējais) privātums;
2) personas fiziskā, psiholoģiskā vai morālā integritāte un
3) personas identitāte un autonomija.[206]

Sejas atpazīšanas tehnoloģiju ietekme uz mūsu tiesībām uz privātumu un mūsu psiholoģisko integritāti ir acīmredzama. Tajā pašā laikā arī cita veida mūsu personiskās dzīves aspektu, piemēram, uzvedības un atrašanās vietas datu, izsekošana un analīze var radīt tādu pašu ietekmi uz mūsu privātumu. Citi mākslīgā intelekta biometriskās atpazīšanas veidi, kas ietver mūsu uzvedības un emociju analizēšanu un prognozēšanu, izmantojot sejas mikroizteiksmes, balss toni, gaitu, sirdsdarbības ātrumu, vēl vairāk ietekmē mūsu psiholoģisko integritāti, dziļi iejaucas mūsu personiskajā sfērā un būtiski ierobežo spēju brīvi paust mūsu personību.

Pirmām kārtām ir svarīgi atcerēties, ka nepastāv zinātniski pierādījumi, kas apstiprina, ka personas iekšējās emocijas var tikt precīzi "nolasītas" no sejas

202 Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif: Stanford Law Books.

203 EST 2013. gada 17. oktobra spriedums lietā C-291/12 *M. Schwarz* pret *Stadt Bochum*, ECLI:EU:C:2013:670, 22., 48.–49. punkts.

204 ECT 2016. gada 12. janvāra spriedums lietā 37138/14 *Szabó and Vissy v. Hungary*, 56. punkts.

205 European Court of Human Rights (2020), Guide on Article 8 of the Convention, p. 40.

206 Ibid., p. 23.

mikroizteiksmēm, sirdsdarbības ātruma vai balss toņa. Nesenos zinātniskos pētījumos ir secināts, ka mākslīgā intelekta emociju uztveršanas sistēmas labākajā gadījumā varētu atpazīt, kā persona subjektīvi interpretē noteiktu citas personas biometrisko iezīmi. Interpretācija neatbilst tam, kā šī persona faktiski jūtas, un mākslīgais intelekts tikai apzīmē šo interpretāciju, kura ir ļoti atkarīga no konteksta un kultūras. Apgalvojumiem, ka mākslīgais intelekts varētu noteikt, piemēram, vai kāds gūs panākumus darbā vai arī ir bīstams sabiedrībai, pamatojoties uz mikroizteiksmēm vai balss toni, nav nekāda zinātniska pamata.[207] Mākslīgā intelekta sistēmu izmantošana biometriskajai identifikācijai un emociju atpazīšanai, piemēram, tiesībaizsardzībā, skolās vai darbā, ietekmē personas fizisko, psiholoģisko un morālo integritāti, kas ir personas privātās dzīves elementi.[208] Turklāt šādas tehnoloģijas aizskar arī citas pamattiesības.

2.3. Diskriminācijas aizlieguma princips

Diskriminācija ir tad, kad salīdzināmā situācijā pret vienu personu izturas mazāk labvēlīgi nekā pret citu, pamatojoties uz uztvertu vai reālu personisko pazīmi vai pazīmēm, kas ir tā sauktie "aizsargātie pamati jeb īpašības".

Hartas 21. pants aizliedz jebkāda veida diskrimināciju, tostarp diskrimināciju dzimuma, rases, ādas krāsas, etniskās vai sociālās izcelsmes, ģenētisko īpatnību, valodas, reliģijas vai pārliecības, politisko vai jebkuru citu uzskatu dēļ, diskrimināciju saistībā ar piederību pie nacionālās minoritātes, diskrimināciju īpašuma, izcelsmes, invaliditātes, vecuma vai dzimumorientācijas dēļ.

Diskriminācijas aizliegums ir noteikts ECTK 14. pantā, kas paredz, ka šajā konvencijā noteiktās tiesības un brīvības ir īstenojamas bez jebkādas diskriminācijas, tālāk uzskaitot aizsargātās pazīmes. ECTK 12. protokols nosaka, ka "jebkuru likumā paredzēto tiesību īstenošana ir nodrošināma bez jebkādas diskriminācijas", sniedzot vēl plašāku aizsargāto pamatu uzskaitījumu, kā arī tas paredz, ka nevienu nevar pakļaut diskriminācijai no publisko institūciju puses uz jebkāda pamata (1. pants).

Minēto normu formulējums izveido neizsmeļamu jeb atvērtu "aizsargāto pamatu" sarakstu, kas tādējādi var tikt attiecināts uz jaunām pazīmēm. Turklāt

207 Feldman Barrett, L., Adolphs, R., Marsella, S., et al. (2019). Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements. *Psychological Science in the Public Interest*, 20(1), pp. 1–68. https://doi.org/10.1177/1529100619832930

208 Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence – Council of Europe. Ad Hoc Committee on Artificial Intelligence (CAHAI). (2020). The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law. Report by Muller, C. https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da

Hartā atšķirībā no ECTK diskriminācijas aizliegums ir noteikts kā patstāvīgas tiesības, uz kurām var atsaukties neatkarīgi no citu tiesību īstenošanas. Minētās tiesības ir saistītas ar Hartas 20. pantā noteikto vienlīdzības principu, kas paredz, ka visas personas ir vienlīdzīgas likuma priekšā.

Saskaņā ar ECTK un ES tiesību aktiem ir iespējams pamatot atšķirīgu vai mazāk labvēlīgu attieksmi. Atšķirīga attieksme var tikt attaisnota, ja tai ir leģitīms mērķis un ja līdzekļi šī mērķa sasniegšanai ir vajadzīgi un samērīgi. Šīs robežas var atšķirties katrā konkrētajā gadījumā atkarībā no apstākļiem. Saskaņā ar ECT judikatūru atšķirīgu attieksmi, kas saistīta ar tādiem jautājumiem, kuri ir personas cieņas pamatā, piemēram, rasi vai etnisko izcelsmi un dzimumu, ir grūtāk pamatot nekā citus gadījumus.[209]

Pieņemot algoritmiskos lēmumus, kas saistīti ar datu izmantošanu, diskriminācija var rasties dažādu iemeslu dēļ, piemēram, to var radīt aizspriedumi, kas apzināti vai neapzināti ir iekļauti sejas atpazīšanas algoritma izveides, testēšanas un ieviešanas laikā, kā arī lēmumi, kādas darbības veikt, pamatojoties uz iegūtajiem rezultātiem. Mākslīgā intelekta sistēmu rezultātus būtiski ietekmē algoritmu vai programmatūras izstrādē izmantoto datu kvalitāte, kas var atspoguļot neobjektivitāti, neprecizitātes un kļūdas datu vākšanas procesā. Lai sejas atpazīšanas programmatūra būtu efektīva un precīza, tā "jāapmāca" ar lielu daudzumu sejas attēlu. Jo vairāk sejas attēlu, jo precīzākas prognozes. Turklāt precizitāti nosaka ne tikai apstrādāto sejas attēlu daudzums, bet arī to kvalitāte. Datu kvalitātei nepieciešams arī seju attēlu kopums, kas ietver dažādas cilvēku grupas. Tomēr daudzos gadījumos algoritmu izveidei tiek vairāk izmantoti baltādaino vīriešu sejas attēli, mazāk – sieviešu un citas etniskās izcelsmes personu attēli. Tāpēc sejas atpazīšanas sistēmas labi darbojas attiecībā uz baltādainiem vīriešiem, bet ievērojami sliktāk tās atpazīst melnādainos iedzīvotājus un sievietes.[210] Salīdzinot personu sejas attēlu ar attēliem datubāzē vai novērošanas sarakstā, ir lielāka kļūdas iespējamība jeb t. s. kļūdaini pozitīvie (*false positive* – angļu val.) gadījumi.

Ir veikti pētījumi, kas pierāda, ka mākslīgā intelekta algoritmi sejas atpazīšanas tehnoloģijās darbojas atšķirīgi atkarībā no personas, kura tiek identificēta,

209 FRA. (2018). Handbook on European non-discrimination law. 2018 edition, p. 93. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-non-discrimination-law-2018_en.pdf

210 Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81, pp. 77–91. http://proceedings.mlr.press/v81/buolamwini18a.html

vecuma, dzimuma vai etniskās piederības.[211] Piemēram, ASV, kur sejas atpazīšanas tehnoloģiju datubāzēs ir vairāk nekā 100 miljoni pieaugušo, sākotnējās datu kopas, kurās lielākoties ir baltādainu un vīriešu dzimuma personu attēli, ietver aizspriedumus pret tumšādainiem cilvēkiem. Sistēmai var būt lielāka kļūdas iespēja attiecībā uz citas ādas krāsas un sieviešu dzimuma personām.[212] Tādējādi šādu grupu pārstāvji var biežāk tikt diskriminēti, piemēram, daudz biežāk nepamatoti apstādināti vai aizturēti. ASV veiktajos pētījumos ir paustas bažas, ka šādas tehnoloģijas var tikt izmantotas, lai kontrolētu un izsekotu visvairāk marginalizētās kopienas un vēl vairāk atstumtu un diskriminētu noteiktas etniskās grupas, kurām jau tāpat ir pievērsta pastiprināta valsts iestāžu uzmanība.[213]

Mākslīgā intelekta uzraudzības sistēmas var radīt īpaši negatīvu ietekmi uz mazāk aizsargātām grupām, piemēram, bērniem, veciem cilvēkiem un cilvēkiem ar invaliditāti. Sejas atpazīšanas precizitāte attiecībā uz bērniem ir ievērojami zemāka.[214] Kļūdainas atbilstības risks palielinās, ja jaunībā uzņemtus sejas attēlus izmanto salīdzināšanai pēc vairāk nekā pieciem gadiem. Tas pats attiecas uz vecāku cilvēku sejas attēliem. Laiks starp attēla uzņemšanu un tā salīdzināšanu negatīvi ietekmē sejas atpazīšanas tehnoloģiju precizitāti.[215] Izvērtējot novērošanas pasākumu ieviešanu un izmantošanu, īpaši ir jāņem vērā bērnu intereses.

2.4. Bērnu tiesības

Bērnu tiesības ir noteiktas Hartas 24. pantā, kura 2. punkts uzsver, ka visās darbībās, kas attiecas uz bērnu, neatkarīgi no tā, vai tās veic valsts iestādes vai privātas iestādes, galvenokārt jāņem vērā bērna intereses. Bērna intereses kā viens no pamatprincipiem ir noteikts arī ANO Bērnu tiesību konvencijā[216], kas pieņemta

211 Sk. EDPB. (2019). Guidelines 3/2019 on processing of personal data through video devices. Version for public consultation. Adopted on 10 July 2019. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf; Wong, Q. (27 March, 2019). Why facial recognition's racial bias problem is so hard to track. *CNET.* https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack/

212 Hardesty, L. (11 February, 2018). Study finds gender and skin-type bias in commercial artificial-intelligence systems. *Massachusetts Institute of Technology.* https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

213 Sk., piemēram, Leslie (2020), Understanding bias in facial recognition technologies.

214 Michalski, D., Yiu, S. Y., & Malec, C. (2018, February). The impact of age and threshold variation on facial recognition algorithm performance using images of children. In: *2018 International Conference on Biometrics* (*ICB*), pp. 217–224, IEEE. https://doi.org/10.1109/ICB2018.2018.00041

215 FRA (2019), Facial recognition technology.

216 Bērnu tiesību konvencija. Pieņemta 20.11.1989. (Latvijā spēkā no 14.05.1992.). *Latvijas Vēstnesis*, 28.11.2014., Nr. 237.

1989. gadā un Latvijā ir spēkā no 2014. gada. Konvencija paredz, ka visās darbībās attiecībā uz bērniem neatkarīgi no tā, vai šīs darbības veic valsts iestādes vai privātas iestādes, kas nodarbojas ar sociālās labklājības jautājumiem, tiesas, administratīvās vai likumdevējas iestādes, primārajam apsvērumam jābūt bērna interesēm (3. panta 1. punkts). Valstij ir jānodrošina bērnam tāda aizsardzība un aprūpe, kas nepieciešama bērna labklājībai un attīstībai.

Bērna interesēm ir jāpievērš primārā uzmanība, attiecinot uz viņiem dažādus mākslīgā intelekta novērošanas pasākumus gan tiešā, gan netiešā veidā. ECT ir uzsvērusi, ka biometrisko datu saglabāšanai, ko veic valsts iestādes par nevainīgām nepilngadīgām personām, var būt īpaši negatīva ietekme, ņemot vērā viņu īpašo situāciju un viņu attīstības un integrācijas sabiedrībā nozīmi.[217] Īpaši būtisks jautājums ir datu vākšana par nepilngadīgajiem valstu robežu pārvaldības nolūkos. Neaizsargātās grupas, to skaitā bēgļi, saskaras ar īpašiem riskiem, jo gadījumā, ja informācija par viņiem nonāktu pie represīvajām valdībām viņu valstīs, šīs personas un viņu ģimenes tiktu pakļautas nopietnam personīgam apdraudējumam.[218]

Arvien biežāk notiek mēģinājumi izmantot sejas un citas biometriskās atpazīšanas tehnoloģijas attiecībā uz bērniem, tomēr līdz šim šos mēģinājumus ir izdevies veiksmīgi apturēt. 2019. gadā Zviedrijas datu aizsardzības iestāde piemēroja pirmo sodu par VDAR pārkāpumu par sejas atpazīšanas tehnoloģiju prettiesisku izmantošanu, lai uzraudzītu skolēnu skolas apmeklējumu.[219] Līdzīgi Francijā divas vidusskolas Nicā un Marseļā sāka izmēģināt sejas atpazīšanas tehnoloģijas, lai kontrolētu apmeklētājus pie skolu ieejas vārtiem, kuras bez maksas nodrošināja ASV tehnoloģiju uzņēmums "Cisco". Pēc nevalstisko organizāciju, skolotāju arodbiedrību un vecāku rīkotas kampaņas projekts tika apturēts un tika lūgts Francijas datu aizsardzības iestādes CNIL atzinums.[220] Iestāde atzina, ka sejas atpazīšanas tehnoloģiju izmēģināšana skolās ir prettiesiska, jo tā pārkāpj datu aizsardzības noteikumus.

Mākslīgā intelekta novērošanas tehnoloģiju ne tikai tieša, bet arī netieša attiecināšana uz bērniem ievērojami aizskar bērnu tiesības. Kā norādīts Apvienoto Nāciju Organizācijas Bērnu fonda (UNICEF) Mākslīgā intelekta politikas vadlīnijās bērniem, bērni un viņu tiesības tiek būtiski ietekmētas ne tikai tad, kad tie

217 ECT 2008. gada 4. decembra spriedums lietās 30562/04 un 30566/04 *Marper v. he United Kingdom*, 124. punkts.

218 Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement.

219 EDPB (22 August, 2019), Facial recognition in school renders Sweden's ..

220 Kayali, L. (29 October, 2019). French privacy watchdog says facial recognition trial in high schools is illegal. *POLITICO.* https://www.politico.eu/article/french-privacy-watchdog-says-facial-recognition-trial-in-high-schools-is-illegal-privacy/

tiek tiešā veidā iesaistīti mākslīgā intelekta novērošanas pasākumu īstenošanā, bet arī kad tas notiek netieši, piemēram, izmantojot novērošanas kameras un prognozējošo modelēšanu. Bērnu labklājība un pilnvērtīgas attīstības iespējas ir ierobežotas, ja augot viņu brīvību un autonomiju pastāvīgi ierobežo mākslīgā intelekta sistēmas, tostarp novērošanas sistēmas.[221] Sagaidāms, ka arvien biežāk būs sastopami mēģinājumi izmantot sejas un cita veida biometriskās atpazīšanas tehnoloģijas, to skaitā arī attiecībā uz bērniem. Tāpēc ir svarīga stipra pilsoniskā sabiedrība, kas būtu gatava aizstāvēt mazāk aizsargāto grupu un personu tiesības.

2.5. Tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu

Mākslīgā intelekta novērošanas tehnoloģijas var ierobežot arī personu tiesības uz taisnīgu tiesu un efektīvu tiesību aizsardzību. Minētās tiesības kā cilvēka pamattiesības ir nostiprinātas gan starptautiskā, gan nacionālā līmenī, sniedzot personām iespēju apstrīdēt pret viņām veiktos pasākumus, lai aizsargātu savas tiesības. Tiesības uz lietas taisnīgu izskatīšanu ir paredzētas ECTK 6. pantā. Tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu ir noteiktas arī Hartas 47. pantā, kas paredz, ka ikvienai personai, kuras tiesības un brīvības, kas garantētas ES tiesībās, tikušas pārkāptas, ir tiesības uz efektīvu tiesību aizsardzību. Satversmes 92. pants nosaka, ka ikviens var aizstāvēt savas tiesības un likumiskās intereses taisnīgā tiesā. Minētais pants tālāk paredz, ka ikviens uzskatāms par nevainīgu, iekams viņa vaina nav atzīta saskaņā ar likumu, kā arī nosaka, ka nepamatota tiesību aizskāruma gadījumā ikvienam ir tiesības uz atbilstīgu atlīdzinājumu. Mākslīgā intelekta sistēmu izmantošana tiesībaizsardzības jomā var radīt bažas par taisnīgas tiesas standartiem, īpaši nevainīguma prezumpciju, tiesībām nekavējoties tikt informētam par aizturēšanas vai apsūdzības iemeslu un būtību, tiesībām uz lietas taisnīgu izskatīšanu un tiesībām sevi aizstāvēt.[222]

Tiesības uz efektīvu tiesisko aizsardzību var tikt pārkāptas, ja valsts iestādes pret personu piemēro piespiedu pasākumus, kuru pamatā ir vienīgi sejas atpazīšanas tehnoloģiju izmantošana vai kurus ir būtiski ietekmējusi šo tehnoloģiju izmantošana, piemēram, policijas apstādināšana vai aizturēšana.[223] Sistēmas

221 UNICEF. (2020). Policy guidance on AI for children. https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

222 Council of Europe. Committee of Experts on Internet Intermediaries (MSI-NET). (2018). Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

223 FRA (2019), Facial recognition technology.

ļoti bieži kļūdās, nosakot, vai persona ir bīstama, un tas savukārt var novest pie nepamatotas aizturēšanas un apcietināšanas, kā arī to izmantošanas rezultātā var tikt apsūdzētas un pat notiesātas nevainīgas personas. Šie apsvērumi bija arī iemesls, kāpēc, piemēram, Kalifornijā šo tehnoloģiju izmantošana tika aizliegta. Proti, pastāv daudz kļūdaini pozitīvu gadījumu, t. i., kad sistēmas ieteiktā iespējamā atbilstība, pārbaudot to cilvēkam, ir izrādījusies nepareiza. Pareizi pozitīvi gadījumi, savukārt, ir sistēmas ieteiktā iespējamā atbilstība, ko operators ir atzinis par pareizu.[224]

Daudzas Apvienotās Karalistes cilvēktiesību aizsardzības organizācijas, piemēram, "Liberty" un "Big Brother Watch", ir paudušas satraukumu, kā arī ir veikti vairāki pētījumi, piemēram, Eseksas Universitātē, kas parāda, ka sejas atpazīšanas tehnoloģijas, ko izmanto policija, nepareizi atpazīst personas, un tas nozīmē, ka nevainīgi cilvēki tiek nepareizi identificēti kā potenciālie noziedznieki.[225] Londonā veiktie astoņi sejas atpazīšanas sistēmu izmēģinājumi no 2016. gada līdz 2018. gadam atklāja, ka 96 % gadījumu programmatūra kļūdaini brīdināja policiju, ka persona atbilst fotoattēlam datubāzē.[226] Kārdifas Universitātes pārskats par Dienvidvelsas policijas sejas atpazīšanas sistēmas izmēģinājumiem 2017. un 2018. gadā atklāja, ka no kopumā 2900 iespējamām atbilstībām, ko konstatēja sistēma, operatori apstiprināja 144 patiesi pozitīvos gadījumus, bet 2756 tika klasificēti kā nepareizi pozitīvi rezultāti.[227] Buenosairesā Argentīnā sejas atpazīšana pilsētas metro sistēmā 2018. gada otrajā ceturksnī izraisīja 1227 brīdinājumus, no kuriem 226 bija patiesi pozitīvi.[228]

Cik daudz no rezultātiem ir kļūdaini pozitīvi, nav precīzi nosakāms. Tomēr, pat ja sejas atpazīšanas sistēmām būtu 99 % precizitāte, kļūdaini pozitīvi rezultāti ir neizbēgami. Ja pastāv 1 % kļūdas īpatsvars, tas nozīmē, ka 100 cilvēki no 10 000 nevainīgiem pilsoņiem tiks atzīti par "meklējamiem".[229]

Viena no galvenajām problēmām ir saistīta ar to, ka tiesībaizsardzību iestāžu novērošanas pasākumu izmantošana un veids, kādā tiek iegūti un izmantoti dati,

224 Lloyd (2020), Information Technology Law, p. 5.

225 Booth, R. (3 July, 2019). Police face calls to end use of facial recognition software. *The Guardian.* https://www.theguardian.com/technology/2019/jul/03/police-face-calls-to-end-use-of-facial-recognition-software

226 Dearden, L. (7 May, 2019). Facial recognition wrongly identifies public as potential criminals 96% of time, figures reveal. *Independent*. https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html

227 Davies, B., Innes, M., Dawson, A. (2018). An evaluation of South Wales Police's use of Automated Facial Recognition. Cardiff University. https://www.statewatch.org/media/documents/news/2018/nov/uk-south-wales-police-facial-recognition-cardiff-uni-eval-11-18.pdf

228 Kayser-Bril (18 June, 2020), At least 11 police forces use face recognition ..

229 Ibid.

ir nepārredzams, kā arī nepastāv efektīvs uzraudzības un kontroles mehānisms. Datu apjoms, ko izmanto tiesībaizsardzības iestādes, var būt milzīgs. Nīderlandē policijai ir piekļuve datubāzei ar 1,3 miljoniem personu attēlu, un daudzas no šīm personām nekad nav apsūdzētas par noziedzīgu nodarījumu.[230] Francijā valsts policija var salīdzināt videonovērošanas videomateriālus ar failu, kas satur 8 miljonus personu attēlu.[231] Veids, kādā darbojas sejas atpazīšanas sistēmas un izstrādātie algoritmi, netiek kontrolēts un uzraudzīts, un šo sistēmu darbība bieži vien ir maz vai pavisam nepārredzama.

Ņemot vērā pārredzamības trūkumu, personu iespējas apstrīdēt tiesībaizsardzības iestāžu pasākumus, kas veikti, pamatojoties uz mākslīgā intelekta sistēmu rezultātiem, var būt ievērojami apgrūtinātas. Personas var nezināt, kas vāc biometriskos datus, vai pat to, ka tie tiek vākti, kā tie tiek glabāti un izmantoti utt. Tiesību uz efektīvu tiesību aizsardzību priekšnosacījums ir, ka personai ir jāapzinās, ka viņas dati ir izmantoti šādās sistēmās, piemēram, ka sejas attēls ir ietverts sejas atpazīšanas sistēmas datubāzē. Eiropas Padomes cilvēktiesību komisārs ir norādījis, ka ikvienam, kurš apgalvo, ka viņš ir publiskas iestādes, privātas organizācijas vai uzņēmuma īstenotas mākslīgā intelekta sistēmas izstrādes, ieviešanas vai izmantošanas upuris, būtu jānodrošina efektīvi tiesiskās aizsardzības līdzekļi. Valstij ir jāgarantē piekļuve efektīviem tiesiskās aizsardzības līdzekļiem tām personām, kurām ir aizdomas, ka pret viņām ir veikti pasākumi, kas pilnībā vai lielā mērā balstās uz mākslīgā intelekta sistēmas sniegto informāciju, nepārredzamā veidā un bez viņu ziņas.[232] Šīs aizsardzības garantijas detalizētāk analizētas grāmatas piektajā un septītajā nodaļā, apskatot Eiropas tiesu praksi un sniedzot politikas rekomendācijas.

Šo tehnoloģiju izmantošana var novest pie personu nepamatotas apsūdzēšanas vai tā sauktās "linča tiesas" arī tad, ja tās izmanto privātie uzņēmumi kādu labu nolūku vadīti. Piemēram, Baltkrievijas izstrādātāji paziņoja, ka strādā pie mākslīgā intelekta algoritma, kas ļauj atpazīt sejas, tādējādi ļaujot atmaskot Minskas nemieru policijas (OMON) darbiniekus, kas bijuši vardarbīgi pret mierīgiem protestētājiem, lai gan viņi ir maskās. Lai arī paziņojums par šādu iespēju izpelnījās lielu popularitāti medijos, tomēr izrādījās, ka šīs tehnoloģijas nepareizi

230 Dutch police facial recognition database includes 1.3 million people. (22 July, 2019). *DutchNews.* https://www.dutchnews.nl/news/2019/07/dutch-police-facial-recognition-database-includes-1-3-million-people/

231 Our legal action against the use of facial recognition by the French police. (21 September, 2020). La *Quadrature du Net.* https://www.laquadrature.net/en/2020/09/21/our-legal-action-against-the-use-of-facial-recognition-by-the-french-police/

232 Council of Europe Commissioner for Human Rights. (2019). Unboxing Artificial Intelligence: 10 steps to protect Human Rights. Recommendation. https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

identificēja vairākus vīriešus, kas nebija policijas darbinieki, kā arī izplatīja šo nepatieso informāciju publiski, bet vairāki policijas darbinieki, kuri, kā tika apgalvots, tika identificēti ar sejas atpazīšanas tehnoloģijām, bija jau nedēļu iepriekš identificēti.[233] Tas vēlreiz parāda, ka šo tehnoloģiju izmantošanu nevar uzskatīt par kādu burvju nūjiņu un nav pieļaujama nekritiska to ieviešana un izmantošana. Mākslīgā intelekta tehnoloģijas nav universāls brīnumlīdzeklis. Tāpēc ir svarīgi noteikt aizsardzības garantijas un izmantošanas robežas, lai novērstu to radīto negatīvo ietekmi, to skaitā novērstu politisko brīvību ierobežošanu.

2.6. Vārda un izteiksmes brīvība, pulcēšanās un biedrošanās brīvība

Tiesības uz vārda un informācijas brīvību ir noteiktas Hartas 11. pantā, kas paredz, ka ikvienai personai ir tiesības uz vārda brīvību un tās ietver uzskatu brīvību un brīvību saņemt un izplatīt informāciju vai idejas bez valsts iestāžu iejaukšanās un neatkarīgi no valstu robežām. Hartas 11. pantā noteiktās tiesības atbilst ECTK 10. pantā noteiktajām tiesībām uz izteiksmes brīvību. ECTK 10. panta 2. punkts nosaka: "Tā kā šo brīvību īstenošana ir saistīta ar pienākumiem un atbildību, tā var tikt pakļauta tādām prasībām, nosacījumiem, ierobežojumiem vai sodiem, kas paredzēti likumā un nepieciešami demokrātiskā sabiedrībā, lai aizsargātu valsts drošības, teritoriālās vienotības vai sabiedriskās drošības intereses, nepieļautu nekārtības vai noziedzīgus nodarījumus, aizsargātu veselību vai tikumību, aizsargātu citu cilvēku cieņu vai tiesības, nepieļautu konfidenciālas informācijas izpaušanu vai lai saglabātu tiesu varas autoritāti un objektivitāti."

Satversmes 100. pants paredz: "Ikvienam ir tiesības uz vārda brīvību, kas ietver tiesības brīvi iegūt, paturēt un izplatīt informāciju, paust savus uzskatus. Cenzūra ir aizliegta."

Var pastāvēt konflikts starp tiesībām uz privātumu un datu aizsardzību, no vienas puses, un vārda un izteiksmes brīvību, no otras puses. Tas ir risināts neskaitāmās Eiropas tiesvedības lietās, it īpaši saistībā ar privātas informācijas paušanu medijos. Kad informācija var apdraudēt būtiskas sabiedrības intereses, piemēram, valsts drošību, sabiedrībai var būt interese ierobežot izteiksmes brīvību, tostarp analizējot, kontrolējot un dzēšot saturu, piemēram, naida runu. Attīstot mākslīgā intelekta sistēmu spējas labāk saprast, analizēt un atklāt naida runu un pamudināšanu uz vardarbību vēlēšanu laikā, var arī palīdzēt aizsargāt

233 Aris, B. (25 September, 2020). Belarus IT specialists develope software to identify OMON officers waring masks. *bne IntelliNews.* https://www.intellinews.com/belarus-it-specialists-develop-software-to-identify-omon-officers-wearing-masks-192747/

politisko līdzdalību. Tajā pašā laikā mākslīgo intelektu var izmantot arī pretēji, lai analizētu un kontrolētu, kādu informāciju iedzīvotāji saņem, ietekmētu politiskos uzskatus un vēlēšanu rezultātus, kā to spilgti parādīja "Cambridge Analytica" skandāls. Šādā gadījumā līdzās tiesībām uz privātumu tiek aizskarta arī uzskatu brīvība.

Mākslīgā intelekta sistēmas var pārkāpt arī tiesības uz pulcēšanās un biedrošanās brīvību, kas ir noteikta Hartas 12. pantā. Minētais pants atbilst ECTK 11. pantam, kas arī paredz, ka jebkuram cilvēkam ir tiesības uz pulcēšanās un biedrošanās brīvību. Šīs tiesības var ierobežot tikai izņēmuma gadījumā. ECTK 11. panta 2. punkts paredz, ka šo tiesību izmantošanu nedrīkst pakļaut nekādiem ierobežojumiem, izņemot tiem, kas noteikti ar likumu un ir nepieciešami demokrātiskā sabiedrībā, lai aizstāvētu valsts vai sabiedrības drošības intereses, nepieļautu nekārtības vai noziegumus, aizsargātu veselību vai morāli, vai citu cilvēku tiesības un brīvības. Saskaņā ar ECTK 15. panta 1. punktu ārkārtēja sabiedriska stāvokļa gadījumā, kas apdraud nācijas dzīvi, valsts var veikt pasākumus, kas atkāpjas no ECTK ietvaros uzņemtajām saistībām tiktāl, cik to nenovēršami prasa situācijas ārkārtas raksturs, ar nosacījumu, ka šie pasākumi nav pretrunā ar citām starptautisko tiesību noteiktajām saistībām. Satversmes 103. pants nosaka, ka valsts aizsargā iepriekš pieteiktu miermīlīgu sapulču un gājienu, kā arī piketu brīvību.

Tādu novērošanas pasākumu kā sejas atpazīšanas izmantošana sabiedriskās vietās var ierobežot personas tiesības brīvi paust savus uzskatus un viedokli, kā arī pulcēšanās un biedrošanās brīvību. Šo tiesību izmantošanas nepieciešams aspekts ir grupas anonimitāte.[234] Sabiedrisku vietu novērošana ar sejas atpazīšanas tehnoloģijām var radīt atturošu efektu un likt cilvēkiem mainīt savu uzvedību. Līdzīgi ir arī gadījumā, ja valsts iestādes novēro personu darbības internetā, piemēram, ierakstus sociālajos medijos. Ja personai ir pamats baidīties, ka viņas paustais viedoklis var radīt kādas negatīvas sekas, viņa var atturēties to paust. Tādējādi tiek aizskarta personas vārda brīvība.[235]

Sabiedrības masveida novērošanas pasākumi tiešā veidā var ierobežot pulcēšanās un biedrošanās brīvību. Sejas atpazīšanas tehnoloģijas sabiedriskās vietās var negatīvi ietekmēt protestētāju vēlmi iesaistīties aktīvismā. Tās var atturēt cilvēkus apmeklēt demonstrācijas, kas ne tikai ir pretrunā ar viņu vārda brīvību, bet arī nopietni ietekmē pulcēšanās brīvību.[236] Spēju iesaistīties šādās darbībās aizsargā Harta un ECTK. Mierīgas pulcēšanās tiesības cilvēkiem dod iespēju kopīgi piedalīties savas sabiedrības veidošanā ietekmīgā, bet mierīgā veidā. Pulcēšanās brīvība aizsargā cilvēku spēju īstenot autonomiju, vienlaikus solidarizējoties ar

234 FRA (2019), Facial recognition technology.

235 UN Human Rights Council (2019), Surveillance and human rights.

236 FRA (2019), Facial recognition technology.

citiem. Sejas atpazīšanas tehnoloģiju ieviešana var radīt atturošu efektu. Personas var atturēties likumīgi īstenot pulcēšanās un biedrošanās brīvību un iesaistīties pilsoniskās līdzdalības aktivitātēs, baidoties no negatīvajām sekām, kas varētu rasties.[237] Tādējādi personas var atturēt no tikšanās ar konkrētām personām vai dalības organizācijās, sanāksmēs un demonstrācijās. Šim atturošajam efektam ir skaidra ietekme arī uz līdzdalības demokrātijas efektīvu darbību.

Vēl pirms Covid-19 vīrusa parādīšanās protestētāji Honkongā aizklāja sejas ar aizsegiem, lai aizsargātos nevis pret vīrusiem, bet lai viņas neatpazītu sejas atpazīšanas tehnoloģijas. Cilvēki, protestējot pret masveida novērošanu un viņu tiesību ierobežošanu, nogāza publiskā vietā uzstādītās videonovērošanas kameras, kas aprīkotas ar sejas atpazīšanas tehnoloģijām. Arī Serbijā Belgradā policija pret protestētājiem izmantoja sejas atpazīšanas tehnoloģijas.[238] Daudzās valstīs, piemēram, Slovēnijā, policijas iestādes izvairās publiski darīt zināmu jebkādu informāciju par šo tehnoloģiju izmantošanu, tāpat kā par citām ar to saistītām darbībām, piemēram, fotogrāfiju vākšanu un sociālo mediju kontu analīzi.[239]

Sejas atpazīšanas tehnoloģijas un citas mākslīgā intelekta biometriskās atpazīšanas tehnoloģijas rada riskus ne tikai cilvēktiesībām un drošībai, bet arī apdraudējumu demokrātijai un tiesiskumam. Tiesībām uz vārda un izteiksmes brīvību, kā arī pulcēšanās un biedrošanās brīvību ir ļoti būtiska nozīme demokrātiskā sabiedrībā. Jauno tehnoloģiju izmantošana, kas var nesamērīgi ierobežot un pārkāpt šīs brīvības, apdraud arī demokrātiskas sabiedrības pamatus.

Tendence arvien plašāk izmantot dažādus sabiedrības novērošanas pasākumus ir novērojama krīzes situācijās, kā Covid-19 pandēmijas laikā, un tas neatceļ cilvēktiesību ievērošanas prasību, kā pamatots nodaļas turpinājumā.

2.7. Pienākums ievērot cilvēktiesības krīzes situācijā

Ir labi saprotams, ka pasākumi, kas nepieciešami Covid-19 apkarošanai, neizbēgami ierobežo personu cilvēktiesības un pamatbrīvības. Ilgstoša piekļuve datiem un sistemātiska personu uzraudzība plašā mērogā, izmantojot tādas digitālās tehnoloģijas kā kontaktu izsekošanas lietotnes, ierobežo tiesības uz privātumu un datu aizsardzību.

237 Fussey, P., Murray, D. (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex, Human Rights Centre, p. 36. https://repository.essex.ac.uk/24946/

238 Serbia: Violent police crackdown against COVID-19 lockdown protesters must stop. (9 July, 2020). *Amnesty International*. https://www.amnesty.org/en/latest/news/2020/07/serbia-violent-police-crackdown-against-covid-19-lockdown-protesters-must-stop/

239 Kučić (7 July, 2020), Slovenian police acquires automated tools ..

Pastāv absolūtas cilvēktiesības, kuras nekādā gadījumā nevar ierobežot, piemēram, tiesības uz dzīvību. Tajā pašā laikā lielākā daļa cilvēktiesību, tostarp tiesības uz brīvību, tiesības uz privātumu, tiesības uz datu aizsardzību, var ierobežot, tomēr ievērojot noteiktus nosacījumus.

Saskaņā ar ECTK tādas intereses kā veselības aizsardzība un sabiedrības drošība ir pamats, lai varētu ierobežot cilvēktiesības, tomēr šādi ierobežojumi ir pieļaujami, ja tie ir "paredzēti likumā" un ir "nepieciešami demokrātiskā sabiedrībā" konkrēta mērķa sasniegšanai (8.–11. panta otrie punkti). Pēdējais nosacījums arī paredz, ka iejaukšanās tiesībās ir jābūt proporcionālai izvirzītajam leģitīmajam mērķim un ka ir piemērots vismazāk ierobežojošais līdzeklis šī mērķa sasniegšanai.[240] Minētie ierobežošanas nosacījumi atrodami arī citos cilvēktiesību dokumentos un ir atsevišķi analizēti grāmatas piektajā nodaļā.

Lai gan ārkārtas situācijās ierobežojumi var tikt piemēroti, pamatojoties uz parasto cilvēktiesību ierobežošanas kārtību veselības aizsardzības interesēs, valstīm ārkārtējā stāvokļa gadījumā var būt jāpieņem arī ārkārtas rakstura pasākumi, kuriem būtu nepieciešamas atkāpes no pienākuma ievērot noteiktas tiesības saskaņā ar starptautiskajiem cilvēktiesību dokumentiem. Šāda iespēja ir noteikta ECTK 15. pantā, un to piemēroja arī Latvija[241] un Igaunija. Šādas atkāpes tiek atzītas par pieļaujamu veidu, kā rīkoties tādās ārkārtas situācijās kā Covid-19 pandēmija, jo tās palīdz nodrošināt pārredzamību un atbildību.[242] Tomēr nav jāpieņem, ka valstis, kas piemēro šādu atkāpšanos, automātiski pārkāpj cilvēktiesības, savukārt valstis, kas izmanto parastos cilvēktiesību ierobežojumus sabiedrības veselības apsvērumu dēļ, tās nepārkāpj.

Lai gan ārkārtas situācija var attaisnot cilvēktiesības ierobežojošu pasākumu piemērošanu, tomēr tās laikā nevar atkāpties no tiesiskuma un demokrātijas principiem. Minētās atkāpes nekad nevar attaisnot darbības, kuras ir pretrunā ar galvenajām likumības, proporcionalitātes, nepieciešamības un nediskriminācijas prasībām. Kā norāda Eiropas Padome, nepieciešamības princips prasa, lai ārkārtas pasākumi sasniegtu savu mērķi, minimāli mainot parastos noteikumus. Turklāt visos ārkārtas stāvokļa laikā pieņemtajos tiesību aktos jāiekļauj arī skaidri termiņi šo ārkārtas pasākumu ilgumam, jo šāda ārkārtas stāvokļa režīma

240 European Court of Human Rights (2020), Guide on Article 8 of the Convention.

241 Sk. Līce, K., Vītola, L. E. (2020). Deklarācija starptautiskajām cilvēktiesību organizācijām par ārkārtējo situāciju Latvijā. *Jurista Vārds*, 14.04.2020., Nr. 15.

242 Sk. Spadaro, A. (2020). COVID-19: Testing the Limits of Human Rights. *European Journal of Risk Regulation*, 11(2), pp. 317–325. https://doi.org/10.1017/err.2020.27

galvenais mērķis ir ierobežot krīzes attīstību un pēc iespējas ātrāk atgriezties normālā stāvoklī.[243]

Eiropas Padomes ģenerālsekretāre Marija Peicinoviča-Buriča (*Marija Pejčinović Burić*) 2020. gada 7. aprīlī publicēja informatīvo dokumentu 46 tās dalībvalstīm. Tā mērķis ir sniegt valdībām rekomendācijas, kā risināt bezprecedenta un masveida Covid-19 sanitāro krīzi veidā, kas respektē demokrātijas pamatvērtības, tiesiskumu un cilvēktiesības.[244] Eiropas Padomes ģenerālsekretāre norāda, ka galvenais sociālais, politiskais un tiesiskais izaicinājums, ar kuru saskaras Eiropas Padomes dalībvalstis, ir to spēja efektīvi reaģēt uz Covid-19 krīzi, vienlaikus nodrošinot, ka to veiktie pasākumi nemazina patieso ilgtermiņa interesi aizsargāt Eiropas pamatvērtības – cilvēktiesības, demokrātiju un tiesiskumu.[245] Eiropas Padome izveidoja forumu, lai kolektīvi nodrošinātu, ka tiek ievēroti divi būtiski priekšnoteikumi: šie pasākumi ir proporcionāli vīrusa izplatības radītajiem draudiem un ir ierobežoti laikā. Lai gan vīruss iznīcina daudzas dzīvības un to, kas ir svarīgs, nedrīkst ļaut tam iznīcināt pamatvērtības un brīvību.

Digitālās uzraudzības tehnoloģijas var būtiski apdraudēt pamattiesības, īpaši tiesības uz privātumu un datu aizsardzību. Neskatoties uz Covid-19 krīzi, cilvēktiesības ierobežojošiem pasākumiem ir jābūt likumīgiem, nepieciešamiem un proporcionāliem pandēmijas radītajiem draudiem, un ierobežotiem laikā.

Lai ievērotu minētos nosacījumus, ieviešot jaunas uzraudzības tehnoloģijas, kā, piemēram, kontaktu izsekošanas lietotnes, ir jāizvērtē to nepieciešamība, proporcionalitāte un efektivitāte. Kaut arī šīs lietotnes tika ieviestas, lai palīdzētu aizsargāt veselību, šī aizsardzība ir pilnībā atkarīga no to efektivitātes. Noteikt, vai iejaukšanās ir proporcionāla, var nebūt vienkārši, ņemot vērā kompromisus, piemēram, starp efektivitāti un privātumu, pierādījumu trūkumu, kā arī to, ka nav skaidras izpratnes, kādas ir samērīguma prasības.[246] Tomēr, neskatoties uz šīm grūtībām, nebūtu jāizdara izvēle starp efektīvu reaģēšanu uz krīzi un pamattiesību aizsardzību.

Juvāls Noa Harari vērš uzmanību, ka patiesībā pati problēmas sakne ir prasīt, lai cilvēki izvēlas starp privātumu un veselību, jo tā ir maldīga izvēle. Mēs varam un mums vajadzētu baudīt gan privātumu, gan veselību. Mēs varam izvēlēties aizsargāt savu veselību un apturēt koronavīrusa epidēmiju, nevis ieviešot

243 Council of Europe. (2020). Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis. https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40

244 Ibid.

245 Ibid.

246 Nijsingh, N., van Bergen, A., Wild, V. (2020). Applying a Precautionary Approach to Mobile Contact Tracing for COVID-19: The Value of Reversibility. *Journal of Bioethical Inquiry*, 17, pp. 823–827. https://doi.org/10.1007/s11673-020-10004-z

totalitāras uzraudzības režīmus, bet gan dodot pilsoņiem vairāk tiesību un brīvības.[247] Arī Eiropas Datu aizsardzības uzraudzītājs Vojcehs Vjevorovskis (*Wojciech Wiewiórowski*) ir uzsvēris, ka cilvēcei nav jāapņemas panākt kompromisu starp privātumu un datu aizsardzību, no vienas puses, un sabiedrības veselību, no otras puses. Demokrātijām Covid-19 krīzes periodā ir jābūt spējīgām nodrošināt tās abas. Covid-19 uzliesmojums pārbauda mūsu sabiedrības izturību, reaģējot uz šo globālo krīzi un cenšoties ierobežot tās sekas gan īstermiņā, gan ilgtermiņā. Krīzes laikā, kā arī pēc tās pastiprināsies tādas digitālās ekonomikas tendences kā varas un informācijas nelīdzsvarotība starp nedaudziem spēcīgiem spēlētājiem un cilvēkiem, kā arī nepietiekama pārredzamība un atbildība.[248]

Strauji pieaugošā tendence, kas īpaši ir pastiprinājusies Covid-19 krīzes laikā, kad mākslīgā intelekta un cita veida novērošanas tehnoloģijas tiek izmantotas pretēji demokrātiskām pamatvērtībām, apliecina nepieciešamību pēc iespējas ātrāk pieņemt skaidru regulējumu, kas paredzētu atbildību, uzliktu pienākumu valsts iestādēm būt atklātām un informēt sabiedrību par to izmantošanu, kā arī noteiktu šo tehnoloģiju izmantošanas sarkanās līnijas. Lai to panāktu, ir būtiski mēģināt saprast, kā esošais regulējums un garantijas, īpaši privātuma un datu aizsardzības regulējums, ir piemērojamas šīm jaunajām tehnoloģijām, kā tās būtu jāattīsta un jāpapildina. Šim jautājumam veltīta nākamā nodaļa.

247 Harari (20 March, 2020), Yuval Noah Harari: the world after coronavirus.

248 Wiewiórowski, W. (30 April, 2020). Carrying the torch in times of darkness. *EDPS.* https://edps.europa.eu/press-publications/press-news/blog/carrying-torch-times-darkness_en

3. DAĻA

Privātuma nozīme

Privātums un datu aizsardzība vairs nav tikai juridiskos tekstos lietoti termini. Tie ir kļuvuši populāri un bieži dzirdami vārdi jaunākajos ziņu sižetu un žurnālu virsrakstos, īpaši – apskatot tehnoloģiju uzņēmumu liela apjoma datu iegūšanas un izmantošanas bieži vien prettiesisko un patvaļīgo praksi, kā arī jaunu aizskarošu tehnoloģiju ieviešanu gan valsts, gan privātajā sektorā. Tajā pašā laikā rodas jautājumi: kādu labumu sabiedrībai un ikvienam no mums sniedz privātums un kāpēc tas ir nepieciešams. Lai gan tiesības uz privātumu ir ietvertas daudzos cilvēktiesību dokumentos, neviens no tiem nepaskaidro, kas ir privātums un kāpēc tas ir jāaizsargā. Šajā nodaļā apskatītas dažādas teorijas, kas skaidro privātuma nozīmi un tā aizsardzības pamatojumu, un ir atklāts, ka privātumam gan kā cilvēka pamattiesībai, gan kā ētiskai un sociālai vērtībai ir izšķiroša nozīme, lai ierobežotu mākslīgā intelekta masveida novērošanas praksi.

Privātuma definēšana nav vienkāršs uzdevums, jo par šī jēdziena nozīmi, vērtību un darbības jomu domas dalās. Tiesību zinātniece Liliana Edvardsa (*Lilian Edwards*) norāda, ka privātums ir īpaši sarežģīta vērtība un tam ir grūti izstrādāt regulējumu, galvenokārt tāpēc, ka ir maz vienprātības par to, kas tas patiesībā ir.[249] Turklāt daudzi zinātnieki ir arī kritizējuši privātumu. Daži no kritiķiem norāda, ka privātums nav uzskatāms par atsevišķām tiesībām. Filozofe Džūdita Džārvisa Tomsone (*Judith Jarvis Thomson*) 1975. gadā rakstīja, ka vispārsteidzošākais saistībā ar tiesībām uz privāto dzīvi ir tas, ka, šķiet, nevienam nav skaidra priekšstata, kas tas ir, turklāt visas dažādās aizsardzības, uz kurām, mūsuprāt, tiesības uz privātumu attiecas, mēs jau esam iekļāvuši citās tiesībās.[250]

Citi kritiķi, savukārt, atzīst, ka privātums ir ļoti subjektīva vērtība, nevis objektīvs jēdziens, kas ir vienlīdz svarīgs visiem cilvēkiem. Kamēr vieniem tādas mūsdienu privātumu ierobežošanas prakses kā sejas atpazīšanas sistēmas var likties pieņemamas, citi stingri iebilst pret šādu biometrisko datu izmantošanu. Ja privātumu uzskata par individuālām interesēm, to ir grūti līdzsvarot ar tādām sociālajām interesēm, kā, piemēram, drošība, sabiedrības drošība, inovāciju un

249 Edwards, L. (ed.). (2019). *Law, Policy, and the Internet*. Oxford, UK; Portland, Orego: Hart Publishing, p. 51.

250 Sk. Thomson, J. J. (1975). The Right to Privacy. Philosophy and Public Affairs, 4(4), pp. 295–314.

ekonomikas izaugsme.[251] Tomēr alternatīvu pieeju, kas paredz objektīvi novērtēt, kādu kaitējumu – ekonomisku, emocionālu vai cieņas – rada privātuma aizsardzības pasākumu trūkums, ir arī ļoti grūti īstenot.[252]

Lai gan ir daudz kritisku uzskatu, tiesību zinātnieki lielākoties tomēr aizstāv privātumu kā nozīmīgu jēdzienu.

3.1. Tiesības palikt vienam

Pirmie privātuma definēšanas mēģinājumi notika jau 19. gadsimtā, kad divi ASV juristi Semjuels Vorens (*Samuel D. Warren*) un Luijs Brendaiss (*Louis D. Brandeis*) savā slavenajā esejā "Tiesības uz privātumu" (*The Right to Privacy* – angļu val.) apzīmēja privātumu kā "tiesības palikt vienam", ko var iztulkot arī kā "tiesības uz likšanu mierā" (*the right to be let alone* – angļu val.).[253] Šis 1890. gadā "Harvard Law Review" publicētais darbs bieži tiek uzskatīts par visietekmīgāko tiesību pārskata rakstu, kāds jebkad ir publicēts.[254]

Autori darbā vērsa uzmanību, ka politiskās, sociālās un ekonomiskās pārmaiņas nozīmē jaunu tiesību atzīšanu un paplašina esošo kopējo tiesību aizsardzību, lai apmierinātu sabiedrības prasības.[255] Jaunākie izgudrojumi un uzņēmējdarbības metodes liecina par nākamo soli, kas jāsper personas aizsardzībai un indivīda tiesību palikt vienam nodrošināšanai. Vispārējās tiesības (*common law* – angļu val.) parasti nodrošina katram cilvēkam tiesības izlemt, cik daudz viņa domas, izjūtas un emocijas atklāt citiem.[256] Spēkā esošās tiesības nosaka principus, kurus var izmantot, lai aizsargātu indivīda privātumu no pārāk uzmācīgas preses, fotoaparātu vai citu modernu ierīču, kas ieraksta attēlus vai skaņas, īpašniekiem.[257] Vispārējās tiesības ir attīstījušās no fiziskas personas un ķermeņa aizsardzības līdz indivīda domu, emociju un sajūtu aizsardzībai, kas tagad prasa juridisku atzīšanu. Šīs tiesības jau pastāv Lielbritānijā lietās par īpašuma tiesībām, kas ļauj, piemēram, literāru darbu autoriem absolūti kontrolēt to publicēšanu.[258] Tomēr šo

251 Edwards (2019), *Law, Policy, and the Internet*, p. 51; sk. arī Bennett, C. J., Raab, C. D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. (2nd and updated ed.) Cambridge, Mass: MIT Press, p. 8.

252 Edwards (2019), *Law, Policy, and the Internet*, p. 53.

253 Warren, S., Brandais, L. D. (1890). The right to privacy. *Harward Law Review*, 4, pp. 193–220. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

254 Edwards (2019), *Law, Policy, and the Internet*, p. 59.

255 Warren, Brandais (1890), The right to privacy, p. 193.

256 Ibid., p. 198.

257 Ibid., p. 206.

258 Ibid., pp. 199–200.

tiesību pamatā nav īpašuma aizsardzība, bet gan tiesības uz privātumu, tās ir daļa no vispārīgākām personas imunitātes tiesībām – tiesībām uz "personas neaizskaramību".[259] Šīs tiesības nav atkarīgas ne no domu un emociju izteikšanas veida (piemēram, vārdi, zīmes, glezniecība, skulptūra, mūzika), ne no tā, vai tās tiek izteiktas literāros vai mākslinieciskos skaņdarbos vai arī ikdienā.[260] Vienlīdz aizsargājams ir, piemēram, dienasgrāmatas ieraksts un dzejolis. Domas, emocijas un izjūtas ir aizsargājamas vienādi neatkarīgi no tā, vai tās ir izpaustas rakstiski, uzvedībā, sarunā, attieksmē vai sejas izteiksmē.[261] Jebkurā gadījumā indivīdam ir tiesības izlemt, vai tās tiek atklātas sabiedrībai.[262]

Lai gan eseja ir sarakstīta vairāk nekā pirms gadsimta, tajā paustie argumenti mūsdienās šķiet vēl aktuālāki nekā tajā laikā. Vai personai ir jābūt pašai tiesīgai noteikt, cik lielā mērā tiek atklātas domas, emocijas un sajūtas, ir viens no galvenajiem jautājumiem, kas pamato nepieciešamību noteikt jauno biometrisko novērošanas tehnoloģiju, kā sejas atpazīšanas un emociju uztveršanas tehnoloģijas, izmantošanas robežas.

S. Vorena un L. Brendaisa eseja aizsāka privātuma tiesisku atzīšanu ASV, un pakāpeniski tika paplašināta tiesību uz privātumu aizsardzība. Lai gan ASV Konstitūcijā termins "tiesības uz privātumu" neparādās, ASV Augstākā tiesa tās ir atzinusi par konstitucionālām tiesībām. 1928. gadā L. Brendaiss bija kļuvis par Augstākās tiesas tiesnesi, un viņš paziņoja, ka ASV Konstitūcijā ir piešķirtas "tiesības palikt vienam", kas paredz, ka valdības nepamatota iejaukšanās indivīda privātajā dzīvē neatkarīgi no izmantotajiem līdzekļiem jāuzskata par ASV Konstitūcijas ceturtā labojuma pārkāpumu.[263] Konstitūcijas ceturtais labojums regulē valdības novērošanu un novērš patvaļīgu privātuma aizskaršanu.[264] Tomēr, neskatoties uz privātuma tiesību atzīšanu, ASV ir izstrādājusi ierobežotu privātuma aizsardzības sistēmu, un tai trūkst tiesību uz privātumu visaptveroša federāla regulējuma. Atšķirībā no Eiropas Savienības ASV vairāk paļaujas uz industrijas pašregulāciju un parasti atbalsta pozīciju, ka bizness un valdība var brīvi piekļūt datiem, lai garantētu ekonomikas izaugsmi vai valsts drošību.[265]

259 Warren, Brandais (1890), The right to privacy, p. 207.

260 Ibid., pp. 198, 207.

261 Ibid., p. 206.

262 Ibid., pp. 198–199.

263 Monti, A., Wacks, R. (2019). *Protecting Personal Information: The Right to Privacy Reconsidered*. Oxford: Hart Publishing, p. 11. https://doi.org/10.5040/9781509924882

264 Sk. Tokson, M. (2020). The Emerging Principles of Fourth Amendment Privacy. *The George Washington Law Review*, 88(1). https://www.gwlr.org/wp-content/uploads/2020/05/88-Geo.-Wash.-L.-Rev.-1.pdf

265 DeCew, J. (2018). Privacy. In: Zalta, E. N. (ed.). *The Stanford Encyclopedia of Philosophy.* https://plato.stanford.edu/archives/spr2018/entries/privacy/

Privātums tā tradicionālajā aspektā ir skatīts kā personas interese netikt pakļautai nevēlamai uzmanībai no valsts vai trešās personas puses.[266] Tāpat Vorens un Brendaiss ielika pamatu izpratnei, ka privātums ietver arī tiesības kontrolēt informāciju par sevi.[267]

3.2. Tiesības kontrolēt informāciju par sevi

Mūsdienās privātumu primāri aplūko kā tiesības kontrolēt informāciju par sevi. Privātums tiek pamatots kā spēja personai pašai noteikt, kad, kā un cik daudz informācijas tiek atklāts citiem.[268] Uzskats, ka personai ir jāatdod kontrole pār saviem datiem, ir pamatā arī ES datu aizsardzības regulējumam. Saskaņā ar šo uzskatu, mēs vienmēr varam izvēlēties, vai dalīties ar savu personisko informāciju un vai atklāt savu iekšējo būtību citiem. Tomēr šī definīcija nepaskaidro, ko var uzskatīt par personisku informāciju, kuru indivīdam ir tiesības kontrolēt.[269] Ir daudz diskusiju par to, kāda ir šī informācija un kādu iemeslu dēļ tā ir jāaizsargā.

Tiklīdz mēs esam brīvprātīgi dalījušies ar savu personisko informāciju, zaudējam kontroli pār tās turpmāko izmantošanu, bet tas nenozīmē, ka informāciju, ko atklājam konkrētam mērķim, var brīvi izmantot, jo mums joprojām saglabājas zināma kontrole pār to. Tomēr šī teorija neatklāj privātuma aizsardzības nepieciešamības pamatojumu. Vēl jo vairāk, vēsture rāda, ka mūsu tiesības kontrolēt personisko informāciju var viegli atņemt gan valdība, gan privātie uzņēmumi. Turklāt līdz ar informācijas sabiedrības attīstību un lielo tehnoloģiju uzņēmumu varas milzīgo pieaugumu šī kontrole mūsdienās ir kļuvusi par ilūziju.

Daudzi zinātnieki joprojām atbalsta šo šauro viedokli, ierosinot tiesības uz privātumu definēt kā tiesības kontrolēt personisko informāciju un nodrošināt garantijas, lai to aizsargātu.[270] Tomēr tādējādi tiek būtiski sašaurināta to nozīme.

Lai arī izpratne par privātumu kā tiesībām "palikt vienam" ir pievilcīga savā vienkāršībā, tā rada jaunu jautājumu: kāpēc persona vēlas, lai to liek mierā, vai kāpēc tai ir nepieciešams palikt vienai? Līdzīgs jautājums rodas arī attiecībā uz šo teoriju, proti: kāpēc mums ir nepieciešams kontrolēt informāciju par sevi?

266 Van Dijk, et al. (eds.). (2018). *Theory and Practice of the European Convention on Human Rights*. 5th ed. Cambridge; Antwerp; Portland: Intersentia, p. 670.

267 DeCew (2018), Privacy.

268 Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum; Hoven, J. van den, et al. (2014, 2019 ed.). Privacy and Information Technology. In: Zalta, E. N. (ed.), *The Stanford Encyclopedia of Philosophy*. https://plato.stanford.edu/archives/sum2020/entries/it-privacy/

269 Solove, D. J. (2009). *Understanding Privacy*. Cambridge, Massachusetts London, England: Harvard University Press, p. 82.

270 Monti, Wacks (2019), *Protecting Personal Information*, p. 128.

3.3. Cilvēka cieņas un autonomijas būtisks aspekts

Privātuma vērtību galvenokārt pamato divi viedokļi. No vienas puses, tiek uzskatīts, ka privātums ir patstāvīga vērtība un neatņemamas tiesības, kas raksturīgas indivīda kā "cilvēka" pastāvēšanai. Šajā ziņā privātums ir saistīts ar cilvēka cieņu, autonomiju un personību, un tiek uzskatīts, ka privātuma aizskārumi pārkāpj šīs vērtības. No otras puses, privātuma lietderība izpaužas kā dažādu labumu, ko gūst gan indivīdi, gan sabiedrība, veicināšana, kuri rodas no privātuma aizsardzības vai kurus samazina privātuma pārkāpumi, piemēram, valsts iestāžu varas prettiesiska izmantošana.[271]

Pirmo viedokli aizstāv vairāki teorētiķi, uzskatot privātumu par būtisku cilvēka cieņas un autonomijas aspektu.[272] Profesors un datoru drošības speciālists Brūss Šneiers (*Bruce Schneier*) uzsver, ka privātums ir cilvēka pamattiesība, kas raksturīga ikviena cilvēka cieņai.[273]

H. Nisenbauma uzskata, ka attiecības starp privātumu un autonomiju digitālajā kontekstā izpaužas vairākos veidos. Privātums nodrošina autonomiju attiecībā uz mūsu personisko informāciju, un tas arī rada vidi, kurā mēs varam izmantot savu autonomiju, justies brīvi domās un darbībā, kas nebūtu iespējams pastāvīga novērošanas riska apstākļos. Turklāt privātums ļauj mums izdarīt brīvas izvēles un rīkoties brīvi, aizsargājot pret manipulācijām ar mūsu izvēli un rīcību.[274]

Eiropas Savienības Tiesas tiesnese, Latvijas tiesību zinātniece profesore Ineta Ziemele vērš uzmanību, ka mūsu liberālā pasaules redzējuma centrā ir viena pamatvērtība – katra cilvēka cieņa. Šajā ziņā privātums ir būtisks cilvēka cieņas elements. Tā ir nepieciešama cilvēka pašnoteikšanās daļa, kas ir viena no īpašībām, kas virza cilvēka evolūciju. Tādējādi privātums, piešķirot mums mūsu privāto telpu, kā arī ļaujot izpaust mūsu izvēles brīvību un brīvo gribu, ir cieši saistīts ar cilvēka cieņu.[275]

271 Sk. Tzanou, M. (2019). *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*. Oxford: Hart Publishing, p. 8.

272 Bernal, P. (2015). *Internet Privacy Rights Rights to Protect Autonomy*. Cambridge: Cambridge University Press, p. 33. http://dx.doi.org/10.1017/CBO9781107337428

273 Schneier (2016), *Data and Goliath* .., p. 148; sk. arī Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. *Philosophy & Technology*, 29(4), pp. 307–312. https://doi.org/10.1007/s13347-016-0220-8

274 Sk. Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79(119). https://core.ac.uk/download/pdf/267979739.pdf; Nissenbaum (2010), *Privacy in context: Technology, Policy and Integrity of Social life.*

275 Ziemele, I. (31 January, 2020). Opening of the Judicial Year Seminar. The European Convention on Human Rights: Living Instrument at 70 – Science and Technology. https://echr.coe.int/Documents/Speech_20200131_Ziemele_JY_ENG.pdf

Privātums dod mums personisko sfēru, kurā varam brīvi attīstīt savu personību, domāt un veidot savu viedokli. Pasaulē, kur tiek aizsargāts privātums, kur maz pazīstam cits citu, cilvēki var brīvi rīkoties, kā viņi vēlas, jo pastāv mazs sociālais spiediens, kas viņus varētu ierobežot. Privātums atbalsta daudzveidību. Tur, kur cilvēki ir aizsargājuši privāto sfēru, viņiem ir brīvība atšķirties no sabiedrības vairākuma uzskatiem un ideāliem. Jo vairāk mēs cits par citu zinām, jo vairāk mēs varam uzspiest sociālās normas. Tādējādi privātuma vērtību nosaka arī sabiedrības atvērtība. Neiecietīgā sabiedrībā privātums ir ļoti vērtīgs, it īpaši, ja jūs kaut kādā veidā atkāpjaties no vispārpieņemtajām normām.[276]

Viens no izplatītākajiem nepareizajiem uzskatiem par privātumu ir, ka tas palīdz tikai likumpārkāpējiem vai kādam, kam ir kaut kas slēpjams.[277] Tomēr nav nekas slikts dziedāt dušā vai stāstīt intīmus noslēpumus tikai labākajam draugam, bet ne vecākiem vai kolēģiem. Mēs parādām dažādus savus aspektus dažādiem cilvēkiem – draugiem, bērniem, vecākiem – un dažādās dzīves lomās – profesionālajā dzīvē un brīvajā laikā, mēs neatklājam visu savu dzīvi sociālo mediju ziņās.

Mums jāapzinās, ka autonomija un brīva griba ir būtisks nosacījums morālajai rīcības brīvībai.[278] Mēs neesam atbildīgi par sekām, kuras nevarējām izvēlēties vai novērst. J. N. Harari vērš uzmanību, ka būtu naivi domāt, ka neviens nevar veiksmīgi paredzēt un manipulēt ar personas izvēli, jo šī izvēle atspoguļo personas brīvo gribu. Viņš brīdina, ka biotehnoloģijas un informācijas tehnoloģiju revolūcija var ļaut lielo datu algoritmiem daudz labāk par pašu personu izprast tās jūtas un pat domas. Tiklīdz lielākajām interneta kompānijām izdosies dziļāk izprast, kā cilvēki pieņem lēmumus, persona tiks pakļauta precīzām vadītām manipulācijām un propagandai. "Facebook" un "Cambridge Analytica" skandāls bija tikai pirmais brīdinājums.[279]

Iepriekš jau tika norādīts, ka viens no galvenajiem mākslīgā intelekta apdraudējumiem ir algoritmiskā manipulācija, kas rada draudus mūsu autonomijai.[280] Mašīnmācīšanās rīkiem ir arvien lielāka spēja ne tikai prognozēt mūsu izvēles, bet arī ietekmēt emocijas un domas un mainīt paredzamo rīcību, dažkārt pat ietekmējot zemapziņu. Šos rīkus var izmantot, lai manipulētu un kontrolētu ne

276 Donath, J. (2020). Privacy and Public Space. In: *The Social Machine. Design for living online*. https://covid-19.mitpress.mit.edu/pub/8icuynaf

277 Schneier (2016), *Data and Goliath* .., p. 147.

278 Weissman, D. (2018). Autonomy and Free Will: Autonomy and Free Will. *Metaphilosophy*, 49(5), pp. 609–645. https://doi.org/10.1111/meta.12333

279 Harari, Y. N. (14 September, 2018). Yuval Noah Harari: the myth of freedom. *The Guardian.* https://www.theguardian.com/books/2018/sep/14/yuval-noah-harari-the-new-threat-to-liberal-democracy

280 Susser, D., Roessler, B., Nissenbaum, H. (2019). Technology, Autonomy, and Manipulation. *Internet Policy Review,* 8(2). https://doi.org/10.14763/2019.2.1410

tikai ekonomisko izvēli, bet arī sociālo un politisko uzvedību.[281] Vadīšana vai kontrolēšana ārpus mūsu apzinātās izpratnes pārkāpj mūsu autonomiju, spēju saprast un patstāvīgi veidot savu dzīvi.[282]

Oksfordas Interneta institūta profesors Lučāno Florīdi (*Luciano Floridi*) uzskata, ka cilvēka cieņa tiešā veidā pamato tiesību uz privātumu aizsardzību. Cilvēka cieņa ir pamatjēdziens, kas nodrošina ietvaru, kurā piemērojamas un interpretējamas tiesības uz privātumu, kā arī datu aizsardzības noteikumi. Viņš tēlaini salīdzina cilvēkus ar ceļotājiem, kuru dzīvi veido dažāda veida informācija. Cilvēki ir kā ceļotāji, kas atkarīgi no daudziem mūsu dzīves vadītājiem: citiem cilvēkiem, fiziskās pasaules, sabiedrības, kultūras, pasaules, kuru mēs radām, ne tikai tās, kurā mēs sevi atrodam. Šajā ceļojumā mums vajadzētu baudīt tiesības uz aizsardzību un viesmīlību. Katrs no mums ir skaista, bet trausla un ļoti maināma vienība. Mūsu cieņa balstās uz to, ka spējam būt kapteiņi mūsu pašu ceļojumos un saglabāt savu identitāti un izvēles iespējas. Jebkura tehnoloģija vai politika, kas tiecas novērst un mazināt šādu atvērtību, riskē mūs dehumanizēt. Tādējādi cilvēka cieņa nodrošina pamatu tiesībām uz privātumu un individuālu kontroli pār informāciju, kas veido un ietekmē cilvēka dzīvi.[283]

3.4. Aizsardzība pret varas ļaunprātīgu izmantošanu

No cita skatpunkta, privātumam ir būtiska nozīme, lai aizsargātu pret varas ļaunprātīgu izmantošanu un nodrošinātu demokrātijas principu ievērošanu. Privātums ir kā "aizsargs pret valdības apspiešanu un totalitārajiem režīmiem", un tam ir vērtība, jo tas ierobežo apspiešanas spēkus un despotiskus režīmus.[284] Privātuma trūkums tiek pielīdzināts valsts uzraudzībai un uzskatīts par totalitāras valsts pazīmi.[285]

Senajā Grieķijā un Romā privātums tika uzskatīts par "aizdomīgu" un "sociāli kaitīgu", jo tas aizstāv norobežošanos no sabiedrības. Privātums nozīmēja "stāvokli, kad kaut kas tiek atņemts".[286] Saskaņā ar kristietības filozofiju labiem cilvēkiem nav nekā slēpjama ne no Dieva, ne no citiem. Grēku izsūdzēšana

281 Council of Europe (2019). Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes. https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4b

282 Susser, Roessler, Nissenbaum (2019), Technology, Autonomy, and Manipulation.

283 Sk. Floridi (2016), On Human Dignity as a Foundation for the Right to Privacy, pp. 307–312.

284 Sk. Tzanou (2019), *The Fundamental Right to Data Protection*, p. 8.

285 Lloyd (2020), Information Technology Law, p. 3.

286 Tzanou (2019). *The Fundamental Right to Data Protection*, p. 9.

(faktiski – informācijas izpaušana) ir veids, kā grēki tiek atlaisti, lai Dievs piedotu izdarīto. Šo teoriju vēlāk pārņēma tādi republikāņu filozofi kā Žans Žaks Ruso (*Jan Jacques Rouseau*), kuri privātas problēmas uzskatīja par draudiem valdības darbībām un par valsts beigām.[287]

Informācijas privātums kā jēdziens sakņojas kopējās bailēs par individuālo privātumu, ko rada atmiņas par nacistu lietu glabāšanu Otrā pasaules kara un pēckara staļinisma laikā. Rietumu valstīs, kad 20. gadsimta 40. un 50. gados pasaule tika atjaunota, pastāvēja lielas bailes no totālas uzraudzības "lielā brāļa" valsts, ko varēja novērot Vācijā un totalitārajā padomju blokā un kuru savos darbos iemūžināja Džordžs Orvels.[288] Šīs bailes Eiropā vēl joprojām ir spilgtā atmiņā. Tādējādi vēsturiski privātums tiek uzskatīts par brīvības elementu, kas dod tiesības būt brīvam no valsts iejaukšanās.[289] Tas ietver vispārēju iejaukšanās aizliegumu un aizsargā pret varas prettiesisku vai pārmērīgu izmantošanu. Nepieciešamība pēc šāda veida aizsardzības bija pamats, lai pēc Otrā pasaules kara tiesības uz privāto dzīvi nostiprinātu galvenajos cilvēktiesību līgumos.

3.5. Tiesības uz privātumu cilvēktiesību dokumentos un to nozīme citu tiesību aizsardzībā

Privātums ir atzīts par universālām cilvēktiesībām. Tās ir noteiktas galvenajos starptautisko cilvēktiesību dokumentos. ANO Ģenerālā asambleja pieņēma un pasludināja Vispārējo cilvēktiesību deklarāciju, kuras 12. pants nosaka: "Nedrīkst patvaļīgi pārkāpt neviena cilvēka privātās dzīves, ģimenes, mājokļa un korespondences neaizskaramību, ne arī apdraudēt viņa godu un reputāciju. Katram cilvēkam ir tiesības uz likuma aizsardzību pret šādiem pārkāpumiem vai apdraudējumiem."

Līdzīgi SPPPT 17. panta pirmā daļa nosaka: "Nedrīkst patvarīgi vai nelikumīgi iejaukties neviena privātajā vai ģimenes dzīvē, apdraudēt mājas neaizskaramību vai korespondences noslēpumu vai nelikumīgi uzbrukt viņa godam un reputācijai." Minētā panta otrā daļa tālāk paredz: "Ikvienam ir tiesības uz likuma aizsardzību pret šādu iejaukšanos vai šādiem apdraudējumiem."

Eiropas tiesību sistēmā tiesības uz privāto dzīvi ir noteiktas ECTK 8. pantā, kura 1. punkts nosaka: "Ikvienam ir tiesības uz savas privātās un ģimenes dzīves, dzīvokļa un korespondences neaizskaramību." Minētā panta otrā daļa paredz

287 Tzanou (2019). *The Fundamental Right to Data Protection*, p. 9.

288 Edwards (2019), *Law, Policy, and the Internet*, p. 59.

289 Rainey, B., McCormick, P., Ovey, C. (2021). *Jacobs, White, and Ovey: The European Convention on Human Rights*. Oxford University Press, p. 411.

aizliegumu valsts institūcijām traucēt šo tiesību realizāciju, izņemot likumā noteiktos gadījumos un ja tas ir nepieciešami demokrātiskā sabiedrībā, lai īstenotu būtiskākas sabiedrības intereses vai lai aizstāvētu citu personu tiesības un brīvības. Gandrīz katra pasaules valsts kaut kādā veidā atzīst privātumu, vai tas būtu konstitūcijā vai citā regulējumā.

Privātums ir būtisks priekšnoteikums arī citu pamattiesību un pamatbrīvību īstenošanai, piemēram, vārda un izteiksmes brīvības, mierīgas pulcēšanās un biedrošanās brīvības un reliģijas brīvības īstenošanai.[290]

Valsts iestāžu, kā arī uzņēmumu uzraudzības rezultātā cilvēkiem pieejamā privātā telpa samazinās, un tas rada atturošu ietekmi uz cilvēku spēju un vēlmi brīvi izteikties un darboties, tostarp pilsoniskajā jomā, kas ir ļoti būtiska demokrātijai.[291]

Mākslīgā intelekta sistēmas ir veidotas un "barotas" ar datiem. Ja viss, ko kāds saka un dara, tiek izsekots un uzraudzīts, tas atstāj atturošu ietekmi uz to, ko cilvēks saka brīvi, kur tas var brīvi doties un ar ko brīvi tikties. Ja esat disidents, tas ietekmēs jūsu spēju kritizēt valdību. Tā ir autoritāras valdības masveida novērošanas būtība – ka cilvēki paši sevi regulē un cenzē.[292]

Privātuma zaudēšana tieši apdraud pulcēšanās, biedrošanās un izteiksmes brīvību. To, cik daudz privātuma zudums var ietekmēt šo pamattiesību īstenošanu, spilgti parāda privātumu aizskarošu tehnoloģiju (kā sejas atpazīšanas tehnoloģijas un telefonu atrašanās vietas izsekošana) izmantošana, lai identificētu protesta akciju dalībniekus, ko varēja novērot, piemēram, Honkongā un Indijā protestu laikā.[293]

Arī Eiropas demokrātiskās valstīs novērošanas tehnoloģiju izmantošana sabiedriskās vietās var ietekmēt personas uzskatu un vārda brīvību, tostarp tāpēc, ka šīs brīvības izmantošanas obligātais aspekts ir grupas anonimitāte. Apziņa, ka, lai uzraudzītu sabiedriskas vietas, tiek izmantotas sejas atpazīšanas tehnoloģijas, var likt cilvēkiem mainīt uzvedību un atturēt viņus no sava viedokļa paušanas. Tādējādi tiek pārkāpta viņu vārda brīvība. Turklāt, ja cilvēki, zinot, ka viņi tiks novēroti, nevēlas apmeklēt demonstrācijas, tas nopietni ietekmē arī pulcēšanās

290 ES Pamattiesību aģentūra, ECT, EP, EDAU (2018), Rokasgrāmata.

291 EDPS (2018), Opinion 3/2018.

292 Andrews, E. L. (11 June, 2020). Governments Aren't Yet Serious About AI's Risk to Human Rights. *Stanford University Human-Centered Artificial Intelligence.* https://hai.stanford.edu/news/governments-arent-yet-serious-about-ais-risk-human-rights

293 Kelly, E. (21 January, 2020). EU makes move to ban use of facial recognition systems. *Science / Business.* https://sciencebusiness.net/news/eu-makes-move-ban-use-facial-recognition-systems; Ulmer, A., Siddiqui, Z. (17 February, 2020). India's use of facial recognition tech during protests causes stir. *Reuters.* https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ

brīvību. Sejas atpazīšanas tehnoloģiju ieviešana var atturēt cilvēkus no pulcēšanās un biedrošanās, baidoties no iespējamām negatīvajām sekām. Tādējādi tiešā veidā tiek ietekmēta arī līdzdalības demokrātijas efektīva darbība.[294]

3.6. Sabiedrības kopējā vērtība

Privātumu bieži saprot kā tiesības, kas aizsargā "privāto", nevis "publisko" sfēru. Tehnoloģijas ir radikāli mainījušas to, kas mūsu ikdienas dzīvē ir privāts un kas publisks. Tiesību zinātnieku vidū šobrīd arvien populārāks kļūst uzskats, ka privātums ir kolektīvs sociāls labums, kā, piemēram, tīrs gaiss un ūdens.[295]

Vēsturiski cilvēku saskarsme bijusi lokāla un īslaicīga. Tikai tuvumā esošie varēja to redzēt, un reiz izteiktie vārdi laika gaitā pazuda. Šobrīd līdz ar interneta un tehnoloģiju attīstību cilvēku mijiedarbība un citu iespējas to novērot var izplatīties telpā un pastāvēt ilgstoši laikā. Mūsu personiskā, profesionālā un finansiālā mijiedarbība aizvien biežāk notiek tiešsaistē, kur gandrīz viss tiek arhivēts un tādējādi potenciāli pastāvīgi meklējams un publicējams.[296] Atteikšanās no sociālo mediju izmantošanas var šķist aizdomīga, jo pastāv uzskats, ka visi cilvēki vēlas savstarpēji mijiedarboties, izmantojot dažādas lietotnes un platformas.

Informācijas un komunikācijas tehnoloģijas ir mainījušas privātuma jēdzienu. Arvien grūtāk ir atšķirt privāto un publisko. Šķiet pilnīgi acīmredzami, ka pāreja uz mazāku privātumu ir neizbēgama un neapturama. Privātuma vērtība saskaras ar jauniem apdraudējumiem līdz ar interneta pieaugumu, vieglumu, ar kādu tas ļauj iegūt, apstrādāt, koplietot un publicēt privāto informāciju, kā arī ar ātro jauno tehnoloģiju attīstību, kas ļauj veikt uzmācīgas novērošanas darbības.

"Publiskās" un "privātās" sfēras nošķiršana liek skatīt privātumu kā individuālas tiesības, kas pastāv līdzās plašākai sabiedrībai. Šis tradicionālais liberālais uzskats, kas balstās uz personības, individualitātes un autonomijas aizsardzību, neskata privātumu kā "sociālu labumu". Netiek ņemta vērā privātuma plašāka sociālā nozīme.[297] Tomēr, lai gan privātums ietver šos principus, tas ir plašāks.

Privātums kalpo nevis tikai indivīda interesēm, bet arī vispārējiem, sabiedrības un kolektīviem mērķiem.[298] Priscila Rīgena (*Priscilla Regan*) skaidro, ka, ska-

294 Sk. FRA (2019), Facial recognition technology.

295 Edwards (2019), *Law, Policy, and the Internet*, p. 53; sk. arī Tzanou (2019), *The Fundamental Right to Data Protection*, pp. 9–10.

296 Donath (2020), Privacy and Public Space.

297 Sk. Moreham, N. A. (2006). Privacy in Public Places. *Cambridge Law Journal*, 65(3), p. 606. https://doi.org/10.1017/S0008197306007240

298 Regan, P. M. (2009). *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill, NC: The University of North Carolina Press, p. 213, 321.

tot privātumu kā individuālas tiesības, politikas veidotājiem ir jāpanāk līdzsvars starp konkurējošām interesēm vai tiesībām, piemēram, tādām sabiedrības interesēm kā drošības aizsardzība. Tomēr sabiedrībai nav jāizvēlas starp dažādām vērtībām un pamattiesībām, tai ir tiesības uz visu pamattiesību nodrošināšanu. Cilvēkiem nav jāizvēlas starp privātuma un datu aizsardzību, no vienas puses, un nacionālo un sabiedrisko drošību, no otras puses. Tāpat kā sabiedrībai nav jāizvēlas starp veselības aizsardzību un privātumu vai demokrātiju. Valstij, ieviešot atbilstošus valsts vai sabiedrības drošības aizsardzības pasākumus, ir jāaizsargā visas cilvēktiesības.

Privātums ir sabiedriska vērtība, tāpēc ka tā aizsargā indivīdu "sabiedrības labā".[299] Privātums nav tikai individuālas tiesības, tās ir grupas tiesības. Tās vairāk pieder grupai kopumā, nevis katram atsevišķam indivīdam.[300] Visai sabiedrībai, ne tikai indivīdam ir labāk, ja pastāv privātums. Lai gan mēs visi esam ieinteresēti privātuma saglabāšanā, tomēr to var apdraudēt liels daudzums individuālu izvēļu, un to apliecina sociālo mediju platformu un dažāda veida lietotņu arvien plašāka izmantošana.[301]

Viens no biežāk dzirdētajiem satraukuma iemesliem ir, ka jaunās tehnoloģijas piespiedīs mūs atteikties no privātuma. ASV tehnoloģiju giganti kļūst daudz varenāki nekā valstis. Mēs ļaujam tiem piekļūt mūsu personiskajai informācijai, ko nekad nedotu nevienai valsts iestādei, – mēs neļautu valdībai ievietot kameras un mikrofonus savās mājās vai izsekot mūsu atrašanās vietu ierīcēs. Šie tehnoloģiju uzņēmumi iegūst informāciju par lietotājiem, lai prognozētu un ietekmētu mūsu uzvedību. Mēs arvien vairāk un vairāk paļaujamies uz mākslīgā intelekta rezultātiem, kas tiek atlasīti pēc konkrētiem algoritmiem, ņemot vērā mūsu pašu sniegto informāciju par mūsu vēlmēm, interesēm u. tml. Tomēr šī piedāvātā un atlasītā informācija var neparādīt mums vairāk atbilstošu un svarīgāku informāciju. Vēl jo vairāk, mākslīgā intelekta algoritmi var ļaut analizēt, saprast un ietekmēt arī mūsu domas un jūtas. Lielajiem tehnoloģiju uzņēmumiem, piemēram, "Facebook", kas veic profilēšanu reklāmas nolūkos, nav nekādas intereses par katru konkrēto lietotāju, un to darbības ne tik daudz uzreiz tieši aizskar katru no mums personiski, kā tiek mēģināts arvien vairāk atņemt visu lietotāju kā grupas tiesības. Privātums paredz aizsardzību pret šādu manipulāciju, turklāt nevis

299 Solove (2009), *Understanding Privacy*, pp. 92–93. Sk. arī Tzanou (2019), *The Fundamental Right to Data Protection*, p. 10.

300 Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy and Technology*, 27, pp. 1–3. https://doi.org/10.1007/s13347-014-0157-8. Vairāk par grupu privātumu sk. Taylor, L., Floridi, L., van der Sloot, B. (eds.). (2017). *Group Privacy: New Challenges of Data Technologies*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8.

301 Edwards (2019), *Law, Policy, and the Internet*, p. 53.

katram no mums atsevišķi, bet kā visu lietotāju grupai. Lai varētu aizsargāt katru no mums atsevišķi, ir jāaizsargā visas sabiedrības kopējās intereses.

Tiesību zinātnieki Lineta Teilore (*Linnet Taylor*), Lučāno Florīdi (*Luciano Floridi*) un Bārts van der Slots (*Bart van der Sloot*) norāda, ka jaunās datu tehnoloģijas, kas ļauj masveidā pārtvert un analizēt datus, kategorizēt cilvēkus bez viņu ziņas un neredzami novērot personu grupu kustību un darbību, rada jautājumus, kuri pārsniedz individuālā privātuma kaitējuma līmeni un rodas grupai gan apzinoties, gan nezinot. Grupas privātumu var uzskatīt par svarīgu individuālā privātuma papildinājumu, un, lai grupas privātums kļūtu par jēdzienu, kam var būt nozīme privātuma un datu aizsardzības tiesībās, mums, iespējams, būtu jāsāk no īpašu problēmu risināšanas. Viena no tām ir masveida novērošana.[302]

Lai demokrātija būtu spēcīga, iedzīvotājiem ir jābūt kontrolei pār saviem personas datiem. Filozofe Karisa Velisa (*Carissa Véliz*) grāmatā "Privātums ir vara" (*Privacy is Power* – angļu val.) uzsver, ka vara, ko privātums mums piešķir kā pilsoņiem, ir nepieciešama demokrātijai – lai mēs varētu balsot atbilstoši savai pārliecībai un bez ietekmēšanas, lai mēs varētu anonīmi protestēt, nebaidoties no sekām, lai mums būtu brīvība apvienoties un paust savas domas. Ja vēlamies dzīvot demokrātijā, varai ir jāpieder cilvēkiem. Un, kam ir dati, tam ir vara. Ja lielākā daļa varas pieder uzņēmumiem, mēs dzīvosim sabiedrībā, kuru pārvalda turīgie. Ja lielākā daļa varas pieder valstij, mums būs sava veida autoritārisms. Lai pārvaldes vara būtu likumīga, tai ir jābalstās uz cilvēku piekrišanu, nevis uz viņu datiem. Liberālā demokrātija nav pašsaprotama, tā ir kaut kas tāds, ar ko mums katru dienu jācīnās. Privātums ir svarīgs, jo tas cilvēkiem dod varu. Privātums ir sabiedrisks labums, un to aizsargāt ir mūsu pilsoniskais pienākums.[303] Tomēr vispirms katram cilvēkam ir jāapzinās, ka viņam šī vara pieder.

3.7. Privātuma nozīmes apzināšanās

Tehnoloģiju uzņēmumi, kas izmanto milzīgus datu apjomus un kļūst arvien spēcīgāki, ir mēģinājuši no jauna definēt privātumu un pārliecināt cilvēkus par privātuma vērtības samazināšanos. Tam pamatā ir peļņa, ko tie gūst, patvaļīgi un neatļauti izmantojot personu datus.

1999. gadā "Sun Microsystems" izpilddirektors Skots Maknīlijs (*Scott McNealy*) atzina: "[Jums] jebkurā gadījumā ir nulle privātuma." Pēc desmit gadiem,

302 Sk. Taylor, L., van der Sloot, B., Floridi, L. (2017). Conclusion: What Do We Know About Group Privacy? In: Linnet, T., Floridi, L., van der Sloot, B. (eds.). *Group Privacy*, pp. 233, 236. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8_12

303 Véliz (2021), *Privacy Is Power*, p. 82.

2010. gadā, šo viedokli dedzīgi atbalstīja divi tehnoloģiju giganti. "Facebook" izpilddirektors Marks Zakerbergs (*Mark Zuckerberg*) skaidroja: "Cilvēki patiešām ir akceptējuši ne tikai dalīšanos ar vairāk un dažāda veida informāciju, bet arī atklātāk un ar vairākiem cilvēkiem. Šī sociālā norma attīstījusies laika gaitā."[304] Tajā pašā gadā "Google" izpilddirektors Ēriks Emersons Šmits (*Eric Emerson Schmidt*) paziņoja: "Ja ir kaut kas tāds, ko nevēlaties, lai kāds zinātu, varbūt jums to nemaz nevajadzētu darīt."[305]

Šo uzņēmumu publiskais vēstījums tagad ir kļuvis gluži pretējs. 2020. gada Pasaules Ekonomikas forumā Davosā Šveicē "Google" izpilddirektors Sundars Pičai (*Sundar Pichai*) apgalvo, ka privātums "nevar būt luksusa prece" un ka atbalsta valdību privātuma regulējumu.[306] Rodas jautājums, kādi notikumi ir noveduši pie šīs attieksmes maiņas.

Galvenais iemesls, kas var ietekmēt privātuma virzienu, ir izpratnes veicināšana par privātumu un personas datu izmantošanu. Atbalsts privātumam vienmēr palielinās, vairāk apzinoties ar privātumu un datu aizsardzības neatļautu izmantošanu un pārkāpumiem saistītos jautājumus. Mēs varam īpaši pateikties tiem cilvēkiem, kuri ir kļuvuši slaveni ar to, ka "izgaismojuši", kā gan valsts institūcijas, gan privātie uzņēmumi, īpaši ASV tehnoloģiju giganti, ļaunprātīgi izmanto personas datus.

Viens no šādiem cilvēkiem, kas būtiski ietekmējis privātuma virzienu, ir Edvards Snoudens, kurš 2013. gada jūlijā atklāja ASV masveida novērošanas programmas neiedomājamos apmēros. Šīs atklāsmes izraisīja globālu sašutumu, kā arī ietekmi uz ES datu aizsardzības sistēmu, paātrinot tās reformu.[307]

Būtiska nozīme stingru datu aizsardzības prasību izstrādē ir EST, kas ir pieņēmusi svarīgus spriedumus lietās, kas ir ietekmējušas datu aizsardzības tiesību attīstību ES. Divas no šādām lietām, kas satricināja visu ES datu nodošanas sistēmu, EST nonāca, pateicoties Maksimiliāna Šrema (*Maximilian Schrems*) iesniegtajām sūdzībām. 2013. gadā viņš iesniedza sūdzību Īrijas datu aizsardzības iestādē

304 The Facebook CEO Chellenges the social norm of Privacy. (12 January, 2010). *Reuters.* https://www.reuters.com/article/urnidgns852573c400693880002576a80069db04/facebook-ceo-challenges-the-social-norm-of-privacy-idUS174222527820100112

305 Jennings, R. (11 December, 2009). Google CEO: if you want privacy, do you have something to hide? *Computerworld*. https://www.computerworld.com/article/2468308/google-ceo--if-you-want-privacy--do-you-have-something-to-hide-.html

306 Google CEO backs GDPR, says privacy should not be a luxury. (22 January, 2020). *The Institute of Engineering & Technology.* https://eandt.theiet.org/content/articles/2020/01/google-ceo-backs-gdpr-says-privacy-should-not-be-a-luxury/

307 Pēc 2013. gada atklājumiem vairāk nekā 1000 akadēmiskās sabiedrības pārstāvju parakstīja dokumentu, lai iebilstu pret masveida novērošanu: Sterling, B. (17 January, 2014). Academics Against Mass Surveillance. *WIRED*. https://www.wired.com/2014/01/academics-mass-surveillance/

par "Facebook" veikto datu nodošanu uz ASV, uzskatot, ka ASV nacionālās drošības regulējums nenodrošina pietiekamu ES pilsoņu personas datu aizsardzību. EST "Schrems I" lietā 2015. gadā atzina par neatbilstošu un spēkā neesošu datu nodošanas mehānismu starp ES un ASV, respektīvi, Eiropas Komisijas lēmumu par aizsardzības līmeņa pietiekamību datu nodošanai uz ASV kā trešo valsti jeb tā saukto drošās zonas lēmumu, ņemot vērā, ka ASV prakse attiecībā uz datu iegūšanu no privātiem uzņēmumiem nacionālās drošības nolūkos nav atbilstoša Hartai. 2020. gada 16. jūlija spriedumā "Schrems II" lietā EST izvērtēja Eiropas Komisijas 2016. gadā pieņemto jauno atbilstības lēmumu 2016/1250 jeb tā saukto ASV un ES privātuma vairogu (*EU-U.S. Privacy Shield* – angļu val.) un atkārtoti atzina lēmumu par spēkā neesošu, ņemot vērā ASV novērošanas regulējumu. Minētās lietas detalizētāk aplūkotas grāmatas piektajā nodaļā.

Iespējams, vēl vairāk privātuma apzināšanos, kā arī nepieciešamību pēc jauna tiesiskā regulējuma veicināja "Facebook" un "Cambridge Analytica" skandāls. Ja Snoudena atklājumi parādīja, kādā veidā valsts iestādes var prettiesiski izmantot personu datus, tad "Cambridge Analytica" skandāls atklāja, cik negatīvas sekas var radīt lielo tehnoloģiju uzņēmumu un sociālo mediju veiktā personas datu apstrāde, ja tā netiek regulēta un uzraudzīta. Apvienotajā Karalistē reģistrēts datu profilēšanas uzņēmums "Cambridge Analytica" 2018. gada sākumā bez piekrišanas izmantoja miljoniem "Facebook" lietotāju datus, lai ar konkrētai auditorijai mērķētām politiskām reklāmām ietekmētu vēlētāju izvēli, to skaitā 2016. gada *Brexit* referenduma kampaņas un ASV prezidenta Donalda Trampa (*Donald John Trump*) priekšvēlēšanu kampaņas laikā. Šie notikumi skaidri parādīja, cik būtisku kaitējumu demokrātijai un sabiedrībai var nodarīt dezinformācija sociālajos medijos, izplatot nepatiesu, neprecīzu un maldinošu informāciju, lai ietekmētu iedzīvotāju politiskos, kā arī cita veida uzskatus un izvēles.[308]

Pēc šī skandāla sabiedrība arvien uzstājīgāk sāka pieprasīt sociālo mediju gigantu atbildību, datu aizsardzības prasību ievērošanu, pārredzamu un viegli saprotamu lietotāju informēšanu par datu apstrādi utt. Eiropas Komisija izveidoja speciālo komisiju, lai izskatītu "Cambridge Analytica" lietu un vairākkārt nopratināja Marku Zakerbergu. "Facebook" apliecināja, ka aptuveni 2,7 miljonu Eiropas iedzīvotāju dati ir izmantoti saistībā ar šo skandālu. Apvienotās Karalistes datu aizsardzības uzraudzības iestāde ICO piemēroja 500 000 eiro naudas sodu, ko

308 Marsden, C., Meyer, T. European Parliament. Panel for the Future of Science and Technology. European Science Media-Hub. (2019). Regulating Disinformation with Artificial Intelligence: Effects of Disinformation Initiatives on Freedom of Expression and Media Pluralism. European Union. https://data.europa.eu/doi/10.2861/003689

"Facebook" piekrita samaksāt.[309] Itālijas uzraudzības iestāde savukārt piemēroja sociālo mediju milzim sodu viena miljona eiro apmērā.[310] Aktīvi tiek meklēti risinājumi un izvērtēti jauna tiesiskā regulējuma priekšlikumi, lai sociālajos medijos cīnītos pret dezinformāciju un nepieļautu turpmāku manipulāciju ar vēlēšanām.

Līdzās arvien pieaugošajai milzīgo tehnoloģiju uzņēmumu varai būtiskākais privātumu apdraudošais aspekts ir jaunās uz datu analīzi balstītās tehnoloģijas, īpaši novērošanas tehnoloģijas. Bieži vien var dzirdēt satraukumu, ka jaunās tehnoloģijas, kā mākslīgais intelekts un lietu internets, piespiedīs mūs atteikties no privātuma. Visplašākās diskusijas ir radījušas jau iepriekš aplūkotās sejas atpazīšanas tehnoloģijas.

Ja līdz šim privātuma un datu aizsardzības prasības bieži vien tika uztvertas negatīvi, norādot, ka tās kavē un traucē tehnoloģiju attīstību, līdz ar sabiedrības arvien plašāku uzmanību un interesi arī uzņēmumu attieksme pret regulējumu ir mainījusies. Tehnoloģiju uzņēmumu darbības pamatā ir patērētāju uzticība. Ja pakalpojumiem un precēm nebūs uzticības, lietotāji tos neiegādāsies un neizmantos. Daudzi lielie tehnoloģiju uzņēmumi ir ne tikai sākuši paust atbalstu privātumam, bet arī paši prasīt valdībām pieņemt regulējumu.[311] Šādas attieksmes maiņas iemesli var būt vēlēšanās stiprināt savu dominanci un varu.[312] Tomēr nav noliedzams – ja vēlas, lai cilvēki izmanto tehnoloģijas, ir jāpanāk, ka viņi tām uzticas. Regulējums ir viena no iespējām, kā šo uzticību iespējams panākt.

3.8. Krīze kā satricinājums privātumam

Nekādi citi notikumi nevar vairāk veicināt jaunu pamattiesības ierobežojošu pasākumu ieviešanu kā krīzes situācijas. Krīzes laikā, kad tiek apdraudētas tādas vērtības kā drošība un veselība, iedzīvotājus ir visvieglāk pārliecināt, ka ir nepieciešams piemērot pasākumus, kas var būtiski ierobežot viņu pamattiesības, tai

309 Statement on an agreement reached between Facebook and the ICO. (30 October, 2019). *WIRED.* https://www.wired-gov.net/wg/news.nsf/articles/Statement+on+an+agreement+reached+between+Facebook+and+the+ICO+30102019151000?open

310 Dobber, T., Fathaigh, R. Ó., Zuiderveen Borgesius, F. J. (2019). The regulation of online political micro-targeting in Europe. *Internet Policy Review*, 8(4). https://doi.org/10.14763/2019.4.1440

311 Nickelsburg, M. (21 January, 2020). Microsoft President Brad Smith calls for AI regulation at Davos. *GeekWire.* https://www.geekwire.com/2020/microsoft-president-brad-smith-calls-ai-regulation-davos/; Sherman, J. (28 Januar, 2020). Oh Sure, Big Tech Wants Regulation—on Its Own Terms. *WIRED.* https://www.wired.com/story/opinion-oh-sure-big-tech-wants-regulationon-its-own-terms/

312 Kharpal, A. (28 January, 2020). Big Tech's calls for more regulation offers a chance for them to increase their power. *CNBC.* https://www.cnbc.com/2020/01/28/big-techs-calls-for-ai-regulation-could-lead-to-more-power.html

skaitā tiesības uz privātumu un datu aizsardzību. Ja vienos svaru kausos tiek likts privātums, bet otros – sabiedrības drošība vai veselība, tie vienmēr nosvērsies par labu otrajiem. Sabiedrība vienmēr būs gatava atteikties no privātuma, lai aizsargātu tādas pamatvajadzības kā drošība un veselība.

Kā norāda Liliana Edvardsa, iespējams, viens no lielākajiem globālajiem izaicinājumiem datu aizsardzībai un privātumam ir baiļu, novērošanas un drošības kultūras veidošanās, ko izraisīja ASV šausminošie 11. septembra terorakti, pēc kuriem NSA ieviesa elektronisko sakaru uzraudzības programmu. Arī Eiropas Savienībā nepieciešamība apkarot terorismu iepriekš bija pamatā datu saglabāšanas režīma ieviešanai, kas ļāva valstīm uzraudzīt sakarus drošības nolūkos. Reaģējot uz teroristu uzbrukumiem vairākās valstīts, ES pieņēma Datu saglabāšanas direktīvu par spīti kritikai, ka tā neatbilst cilvēktiesībām. Direktīva ļāva valstīm uzraudzīt sakarus drošības nolūkā. Pagāja astoņi gadi, līdz šo direktīvu atcēla EST. Vēsturiskā pieredze liecina, ka krīzes un satricinājumu laikā pieņemtus pamattiesības ierobežojošus pasākumus vēlāk ir ļoti grūti atcelt un tas var prasīt ilgu laiku. Lai veicinātu novērošanas kultūras attīstību, tiek izmantoti ne tikai terorakti un drošības draudi.

Lielu pārbaudījumu un satricinājumu visās jomās, to skaitā cilvēktiesībām un privātumam, neapšaubāmi radīja arī Covid-19 pandēmijas izraisītā globālā krīze. Kā atklāja grāmatas pirmajā nodaļā aprakstītie piemēri, sabiedrības bailes par personisko drošību un veselību, kā arī vispārējo haosu, neaizsargātību un nedrošību gan valsts iestādes, gan privātie uzņēmumi izmantoja, lai lielā ātrumā izstrādātu un ieviestu daudzas jaunas digitālās novērošanas tehnoloģijas. Turklāt daudzos gadījumos šīs tehnoloģijas tika ieviestas, neizvērtējot to efektivitāti, nepieciešamību un samērīgumu.

Jautājumus par Covid-19 krīzes laikā piemēroto ierobežojošo pasākumu, tostarp jauno novērošanas tehnoloģiju, risinājumiem, to likumību un atbilstību cilvēktiesībām tiesas izvērtēs vēl ilgi pēc pandēmijas beigām. Lai gan krīzes situācijā ir pieļaujams vairāk ierobežot personu pamattiesības, šādiem ierobežojumiem ir jābūt samērīgiem un pamatotiem, un tie ir jāpārtrauc, tiklīdz situācija uzlabojas. Tajā pašā laikā sagaidāms, ka valsts iestādes un privātais sektors turpinās attīstīt un nevēlēsies atteikties no jau ieviestajām novērošanas tehnoloģijām.

Jebkura krīze nozīmē pārmaiņas. Arī pēc Covid-19 pandēmijas pasaule būs pavisam citāda nekā tā, kurā mēs dzīvojām iepriekš. Nav paredzams, cik daudz Covid-19 krīze izmainīs sabiedrību, kā arī tās ietekmi uz cilvēktiesībām un to ierobežošanu. Tomēr būtu naivi domāt, ka ieviestie cilvēktiesības ierobežojošie, tostarp novērošanas, pasākumi pilnīgi pazudīs un valstis atkal atgriezīsies pie iepriekšējās kārtības. Lai veicinātu pasākumu atbilstību un likumību, vispirms ir svarīgi apzināties to ietekmi uz pamattiesībām, kā arī uz visu sabiedrību un demokrātiju, kā arī pēc tam izstrādāt atbilstošu regulējumu, kas novērstu šo apdraudējumu.

Grāmatā iepriekš atklāts, kā mākslīgā intelekta novērošanas tehnoloģijas ietekmē cilvēktiesības, kā arī demokrātiju un sabiedrību kopumu. Šī nodaļa parāda, ka, lai gan viedokļi par to, kāpēc privātums ir jāaizsargā, ir dažādi un laika gaitā mainās un attīstās, tomēr privātumam ir būtiska un patstāvīga nozīme. Tiesības uz privātumu vēsturiski ir attīstījušās kā būtiskas liberālas tiesības, kas nodrošina aizsardzību pret varas ļaunprātīgu izmantošana; tiesības palikt vienam, tiesības kontrolēt informāciju par sevi – tās ir autonomijas un rīcības brīvības garants. Privātums tiek uztverts arī kā visas sabiedrības kopīga vērtība un kā cilvēka cieņas neatņemams elements, kas kā ētikas pamatvērtība jauno tehnoloģiju laikmetā aizsargā pret visaptverošu novērošanu un varas asimetriju. Tādējādi tiesības uz privātumu ir uzskatāmas gan par pamattiesībām, gan ētikas principu un sabiedrisku vērtību. Tās ir arī būtisks tiesiskuma un demokrātijas elements.

Vēl vienas pamattiesības, ko būtiski ietekmē mākslīgā intelekta novērošanas tehnoloģijas un kas ir cieši saistītas ar tiesībām uz privātumu, ir tiesības uz datu aizsardzību. Šīs abas pamattiesības izvirza konkrētas prasības un aizsardzības garantijas, kas piemērojamas arī mākslīgā intelekta novērošanas sistēmām. Turklāt datu aizsardzības tiesības ir galvenais regulējums, kas jau šobrīd piemērojams attiecībā uz mākslīgā intelekta sistēmām un kas būtiski ietekmē arī topošo mākslīgā intelekta tiesisko regulējumu, kuru šobrīd aktīvi izstrādā gan ES, gan citas starptautiskās organizācijas. Nākamajā nodaļā apskatīta tiesību uz datu aizsardzību tiesiskā regulējuma attīstība, kā arī mākslīgā intelekta regulējuma aizsākumi gan starptautiskā, gan ES līmenī.

4. DAĻA

Datu aizsardzības tiesības un mākslīgā intelekta regulējuma attīstība

Datu aizsardzības aizsākumu pamatā ir tehnoloģiju progress. Līdz ar informācijas sabiedrības un tehnoloģiju attīstību datu aizsardzības tiesības kā patstāvīgas cilvēktiesības pakāpeniski izveidojās no tiesībām uz privāto dzīvi.

Eiropā tās sāka attīstīties 20. gadsimta 70. gadu sākumā, kad līdz ar tehnoloģiju straujo progresu arvien plašāk sāka izmantot datorus un bija nepieciešams izstrādāt noteikumus, kas regulētu personīgās informācijas vākšanu un apstrādi.[313] Mūsdienās datu aizsardzības tiesiskais regulējums ir pieņemts lielākajā daļā pasaules valstu, kā arī daudzās valstīs privātums un datu aizsardzība ir konstitucionāli garantētas tiesības. Kā liecina ANO sniegtā informācija, 132 no 194 valstīm ir pieņēmušas tiesību aktus par datu aizsardzību un privātumu.[314]

Līdzās valstu tiesiskajam regulējumam arī ES un starptautiskā līmenī ir pieņemti daudzi datu aizsardzības tiesiskie instrumenti. Atšķirīgais valstu regulējums un dažādie standarti attiecībā uz datu iegūšanu, izmantošanu un nodošanu radīja būtiskus šķēršļus starptautiskiem uzņēmumiem, tāpēc bija nepieciešams vienoties par starptautiski vienotu risinājumu, kurā tiktu samērotas, no vienas puses, personas tiesības uz datu aizsardzību un, no otras puses, uzņēmumu komerciālās intereses. Izveidojās divas galvenās pieejas, kādā tiek skatītas datu aizsardzības tiesības: 1) ekonomiskā pieeja un 2) cilvēktiesību aizsardzības pieeja.[315] Tās abas apskatītas nodaļas turpinājumā.

Datu aizsardzības regulējums ir attīstījies, mēģinot atrast veidu, kā samērot dažāda veida intereses: uzņēmumu biznesa intereses, īpaši tehnoloģiju nozarē; valsts iestāžu intereses aizsargāt valsts un sabiedrības drošību, kā arī citas sabiedrības intereses; preses un izteiksmes brīvība; publisko iestāžu intereses dalīties ar datiem, lai digitalizētu dažāda veida publiskos pakalpojumus, piemēram, transporta, veselības, nodokļu jomā, utt.[316] Lai gan šajā pētījumā pamatā ir analizēts, kā privātums un datu aizsardzība saduras un ir samērojamas ar valsts un sabiedrības drošības interesēm, piemērojot dažāda veida novērošanas pasākumus, kā šī

313 Rudgard, S. (2018). Origins and Historical Context of Data Protection Law. In: Ustaran, E., Lovells, H. (eds.), *European Data Protection. Law and Practice.* International Association of Privacy Professionals (IAPP), pp. 20, 26.

314 Sk. UNCTAD. Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

315 Tzanou (2019), *The Fundamental Right to Data Protection*, p. 14.

316 Edwards (2019), *Law, Policy, and the Internet*, p. 66.

interešu sadursme attīstās un ir regulējama mākslīgā intelekta laikmetā, tomēr piemērojamais regulējums, kā arī prakse daudzos gadījumos var būt līdzīgā veidā attiecināma, izvērtējot arī citus interešu konfliktus.

Datu aizsardzības tiesības iezīmē sākumu informācijas un komunikāciju tehnoloģiju regulējumam no likumdevēja puses. Tiesiskie instrumenti, kas tika izveidoti, balstoties uz 20. gadsimta 70. un 80. gados definētajiem principiem, vairs nespēja reaģēt uz sociāli tehniskajām izmaiņām. Arvien plašākas datu pārsūtīšanas iespējas, jaunie datu glabāšanas un skaitļošanas resursi, īpaši mākoņdatošana, lielākās daļas mūsu dzīves un vides pakāpeniska datu apstrāde, sevišķi līdz ar lietu interneta pieaugumu, kā arī liela mēroga un prognozējoša datu analīze, pamatojoties uz lielajiem datiem un mašīnmācīšanos, radīja nepieciešamību pēc jauna regulējuma.[317] Lai reaģētu uz šīm pārmaiņām, Eiropā tika veikta datu aizsardzības reforma, kuras rezultātā ES pieņēma VDAR un citus tiesību aktus, kā arī Eiropas Padome modernizēja Konvenciju 108.[318]

Tajā pašā laikā regulējuma izstrādes un pieņemšanas process vienmēr aizņem ilgu laiku, līdz ar to neizbēgami tas nespēj tikt līdzi straujajai tehnoloģiju attīstībai. Kā atklāts grāmatas sestajā nodaļā, jaunais datu aizsardzības regulējums nespēj risināt daudzus izaicinājumus, ko rada mākslīgā intelekta sistēmas un citas jaunās tehnoloģijas un tiešsaistes platformas.

Pēdējo gadu laikā gan starptautiskā un ES, gan nacionālā līmenī ir pieņemti daudzi nesaistoši dokumenti, kas cenšas šo "plaisu" starp regulējumu un tehnoloģiju attīstību novērst, kā arī tiek izstrādāti daudzi priekšlikumi, kā uzlabot esošo regulējumu. Arī privātie uzņēmumi, tehnoloģiju organizācijas un nevalstiskās organizācijas aktīvi iesaistās diskusijās par mākslīgā intelekta sistēmu regulēšanu un ir pieņemtas dažāda veida deklarācijas un vadlīnijas, kas nosaka mākslīgā intelekta principus. Pašregulācija nav pietiekama, lai nodrošinātu, ka privātās organizācijas izstrādā un izmanto mākslīgā intelekta sistēmas ētiski un atbilstoši sabiedrības interesēm, un noteiktu to atbildību. Skaidrs regulējums ir jāpieņem arī attiecībā uz publisko sektoru un privātā un publiskā sektora partnerību. Eiropas un starptautiskās organizācijas šobrīd aktīvi izstrādā jaunu regulējumu, kas paredzētu juridiski saistošas prasības mākslīgā intelekta sistēmām un citām jaunajām tehnoloģijām un platformām.

Nodaļas turpinājumā aplūkots, kā starptautiskās organizācijas – Eiropas Padome, OECD, ANO, UNESCO – ir attīstījušas datu aizsardzības tiesības. Pēc tam aplūkota ES datu aizsardzības regulējuma attīstība, kur tiesības uz datu aizsardzību atšķirībā no citu starptautisko organizāciju pieņemtajiem cilvēktiesību dokumentiem

317 Mantelero (2020), Regulating AI within the Human Rights Framework, p. 484.

318 Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi. Pieņemta 28.01.1981. (EP, Latvijā spēkā no 01.09.2001.). *Latvijas Vēstnesis*, 12.04.2001., Nr. 59.

ir noteiktas kā atsevišķas pamattiesības. Vienlaikus nodaļā sniegts vispārīgs pārskats, kā dažādas organizācijas ir iesaistījušās diskusijā par masveida novērošanas pasākumu apdraudējumu cilvēktiesībām un kā pakāpeniski tiek izveidots mākslīgā intelekta regulējums, apskatot būtiskākās iniciatīvas starptautiskā un ES līmenī.

4.1. Starptautiskās iniciatīvas

4.1.1. Eiropas Padome

Eiropas Padome ir izstrādājusi vienotus Eiropas cilvēktiesību aizsardzības standartus, kā arī radījusi efektīvu to aizsardzības mehānismu.[319] Viens no būtiskākajiem starptautiskajiem cilvēktiesību dokumentiem ir ECTK, kuras ievērošanu uzrauga ECT. 1968. gadā Eiropas Padomes Parlamentārā asambleja uzdeva Ministru komitejai izvērtēt, vai valstu regulējums pietiekami aizsargā tiesības uz privātumu pret pārkāpumiem, ko var radīt moderno zinātņu un tehnoloģiju attīstība, un, ja atbilde ir negatīva, izstrādāt rekomendācijas, lai labāk aizsargātu tiesības uz privātumu.[320] Eiropas Padomes Ministru komiteja pieņēma divas rezolūcijas par datu aizsardzību: 1973. gadā rezolūcija noteica datu aizsardzības principus privātajā sektorā, bet 1974. gada rezolūcija – publiskajā sektorā.[321] Rezolūcijas ieteica nacionālajā likumdošanā ietvert prasības, kas arī tagad lielākoties ir pamatā datu aizsardzības principiem, piemēram, lai dati tiktu iegūti godīgi, lai tiktu nodrošināta to precizitāte un aktualitāte, lai tiktu ievērots datu minimizēšanas princips, kas aizliedz vākt vairāk datus un glabāt tos ilgāk, nekā tas ir nepieciešams, pienākums uzraudzīt to izpaušanu, datu subjektu tiesības utt. Tajā pašā laikā rezolūcijas nenoteica pasākumus, kas valstīm būtu jāveic, lai ieviestu principus nacionālajā likumdošanā. Lai saskaņotu valstu tiesību aktus, kas tika strauji pieņemti,

319 Sk. Pati, R. (2009). Due Process and International Terrorism. Leiden, Boston: Nijhoff, pp. 72, 73; Christoffersen, J. and Madsen, M. R. (2011). Introduction: The European Court of Human Rights between Law and Politics. In: Christoffersen, J. and Madsen, M. R. (eds.), *The European Court of Human Rights between Law and Politics*. Oxford: Oxford University Press, p. 2.

320 Parliamentary Assembly of the Council of Europe. (1968). Recommendation 509. Human rights and modern scientific and technological developments. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en

321 Council of Europe. Committee of Ministers. (1974). Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51; Council of Europe. Committee of Ministers. (1973). Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830

Eiropas Padome uzsāka darbu pie viena no nozīmīgākajiem starptautiskajiem tiesiskajiem instrumentiem.

1981. gadā Eiropas Padome pieņēma Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (Konvencija 108).[322] Šī konvencija ir pirmais un līdz šim brīdim vienīgais juridiski saistošais starptautiskais dokuments datu aizsardzības jomā, kuram var pievienoties ikviena pasaules valsts, arī valstis ārpus Eiropas Padomes. Konvencijai ir pievienojušās 55 valstis – visas Eiropas Padomes dalībvalstis (46 valstis), kā arī to ir ratificējušas vairākas valstis ārpus Eiropas.[323]

Konvencija 108 tika pieņemta, lai nodrošinātu pamattiesību un pamatbrīvību, it īpaši privātās dzīves neaizskaramības, ievērošanu, kā arī regulētu automātiski apstrādāto personas datu plūsmu pāri robežām. Tā attiecas uz datu apstrādi gan valsts, gan privātajā sektorā. Konvencijā ir noteikti datu aizsardzības principi. Tā uzliek pienākumu dalībvalstīm pieņemt atbilstošus datu aizsardzības noteikumus, kā arī nosaka datu aizsardzības likumības un datu kvalitātes principu, pienākumu nodrošināt īpašu kategoriju datu aizsardzību, datu drošības principu un apstrādes pārredzamības principu. Konvencijā 108 ir noteiktas datu subjekta tiesības, tostarp tiesības, lai tiktu ņemts vērā personas viedoklis par automatizētu datu apstrādi, tiesības uz informāciju, tiesības iebilst pret datu apstrādi, tiesības piekļūt, labot un dzēst datus, kā arī izmantot tiesiskās aizsardzības līdzekļus datu aizsardzības pārkāpuma gadījumā. Konvencija uzliek datu pārzinim un apstrādātājam pienākumu veikt atbilstošus pasākumus, lai varētu pierādīt datu apstrādes atbilstību Konvencijai. Tā paredz iespēju atkāpties no noteiktām datu aizsardzības prasībām, ja tas ir paredzēts normatīvajos aktos, tiek ievērota pamattiesību un pamatbrīvību būtība un šāda atkāpšanās ir samērīga un nepieciešama demokrātiskā sabiedrībā, lai aizsargātu tādas sabiedrības intereses kā valsts un sabiedriskā drošība, kā arī datu subjektu vai citu personu tiesības un brīvības. Konvencijā ir regulēta arī pārrobežu personas datu nodošana. 2001. gadā tika veikti Konvencijas labojumi, pieņemot papildu protokolu, kas ieviesa noteikumus par pārrobežu datu plūsmu uz trešajām valstīm un noteica obligātu valsts datu aizsardzības uzraudzības iestāžu izveidošanu.

Eiropas Padome 2011. gadā uzsāka darbu pie Konvencijas 108 modernizēšanas, lai nodrošinātu tās efektivitāti, ņemot vērā informācijas un komunikācijas

322 Vairāk par Konvencijas 108 pieņemšanas procesu sk.: Council of Europe. (1981) Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/16800ca434

323 Līdz 2021. gada jūnijam Konvencijai 108 bija pievienojušās šādas valstis, kas nav ES dalībvalstis: Argentīna, Kaboverde, Maurīcija, Meksika, Maroka, Urugvaja, Senegāla un Tunisija. Sk. Council of Europe. Chart of signatures and ratifications of Treaty 108. Status as of 12/06/2021. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures

tehnoloģiju radītos izaicinājumus privātuma aizsardzībai.[324] Konvencijas 108 modernizēšana tika veikta paralēli ES datu aizsardzības reformai, pēc iespējas nodrošinot tiesiskā regulējuma atbilstību.

2018. gada 18. maijā Eiropas Padome pieņēma protokolu[325], ar ko groza Konvenciju 108, un tas tika atvērts parakstīšanai 2018. gada 25. jūnijā (Konvencija 108+). Protokols nostiprina Konvencijā 108 noteiktos datu aizsardzības principus un ietver papildu aizsardzības pasākumus, lai risinātu problēmas, kas saistītas ar personas datu aizsardzību, ko rada jaunās tehnoloģijas. Modernizētā konvencija ievērojami palielina datu aizsardzības līmeni. Tā nosaka stingrākas prasības attiecībā uz proporcionalitātes principu un datu minimizēšanas principu, datu apstrādes likumību un datu apstrādes pārredzamību. Tā paplašina sensitīvo datu veidus, ietverot arī ģenētiskos un biometriskos datus un datus par etnisko izcelsmi. Konvencija 108+ paredz arī jaunus pienākumus, tostarp ziņot par nopietniem datu pārkāpumiem, un nosaka stingrāku datu pārziņa atbildību, kā arī skaidru pārrobežu datu plūsmas režīmu. Turklāt tā piešķir personām jaunas tiesības algoritmisko lēmumu pieņemšanas kontekstā, kas ir īpaši svarīgi saistībā ar mākslīgā intelekta attīstību. Tā arī paplašina Konsultatīvās komitejas kompetenci, kura uzrauga, vai puses efektīvi īsteno atjauninātā līguma noteikumus. Konvencija 108+ nostiprina datu aizsardzības iestāžu pilnvaras un neatkarību, kā arī uzlabo starptautisko sadarbību.

Konvencijā noteiktie principi saskan un pastiprina ES datu aizsardzības tiesisko regulējumu. Pievienošanās Konvencijai 108 tiek ņemta vērā, vērtējot aizsardzības līmeni valstīs ārpus ES, it īpaši starptautisko datu nosūtīšanas gadījumā.[326]

Saistībā ar jautājumu par personas datu apstrādi valsts drošības un aizsardzības nolūkā Konvencijas 108+ 11. pantā ir iekļauta stingra pārbaudes un līdzsvara (*checks and balance* – angļu val.) sistēma. Konvencija 108+ attiecas uz visu personas datu apstrādi publiskajā un privātajā sektorā, ieskaitot drošības un izlūkošanas dienestus (3. pants). Tā paredz piemērot datu aizsardzības principus visām apstrādes darbībām, arī tām, kas veiktas valsts drošības apsvērumu dēļ, ar

324 Vairāk par Konvencijas 108 modernizēšanu sk. Council of Europe. (2018). Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/16808ac91a

325 Protokols, ar ko groza Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu apstrādi: *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Pieņemts 10.10.2018. https://rm.coe.int/16808ac918; Council of Europe. (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data – Consolidated text. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

326 VDAR Preambulas 105. apsvērums; Council of Europe (2018), Explanatory Report to the Protocol amending ..

iespējamiem izņēmumiem un ierobežojumiem, ievērojot noteiktus nosacījumus, piemēram, neatkarīgu un efektīvu pārskatīšanu un uzraudzību.

Latvijai ir saistošas datu aizsardzības prasības, kas noteiktas starptautiskā līmenī. 2001. gadā Latvija ratificēja Konvenciju 108, pieņemot likumu "Par Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi".[327] 2018. gada 10. oktobrī Latvija parakstīja jauno protokolu un kļuva par vienu no valstīm, kas ir pievienojusies Konvencijai 108+.[328]

Līdzās Konvencijai Eiropas Padome ir pieņēmusi rekomendācijas, rezolūcijas un cita veida dokumentus, kas skaidro Konvencijā noteikto principu interpretāciju un piemērošanu dažādās jomās.[329] Tāpat Eiropas Padome ir pieņēmusi nozīmīgus dokumentus, lai vērstu uzmanību uz masveida novērošanas radīto apdraudējumu cilvēktiesībām. 2015. gadā Eiropas Padomes Ministru komiteja pieņēma Rezolūciju "Par masveida novērošanu".[330] Tā tika pieņemta kā reakcija uz E. Snoudena atklājumiem, vēršot uzmanību, ka atklātā masveida novērošanas prakse apdraud ECTK noteiktās cilvēktiesības, ieskaitot tiesības uz privātumu (8. pants), informācijas un izteiksmes brīvību (10. pants), tiesības uz taisnīgu tiesu (6. pants) un domu, pārliecības un ticības brīvību (9. pants). Šīs tiesības ir demokrātijas stūrakmeņi, un to pārkāpumi bez atbilstošas tiesas kontroles apdraud arī tiesiskumu.[331] Rezolūcijā Ministru komiteja aicināja ES pabeigt darbu pie Vispārīgās datu aizsardzības regulas, kā arī pieņemt atbilstošu regulējumu datu nodošanai uz trešajām valstīm. Savukārt dalībvalstis tika mudinātas pieņemt atbilstošu tiesisko regulējumu, kas attiektos uz izlūkdienestu darbību, kā arī veicināt lietotājam draudzīgu tādu automātisko datu aizsardzības metožu turpmāku attīstību, kas spēj cīnīties pret masveida novērošanu un citiem interneta drošības draudiem, arī ārpus valsts sektora.[332]

2020. gada septembrī Eiropas Padomes Konvencijas 108 Konsultatīvās komitejas priekšsēdētāja Alesandra Pjeruči (*Alessandra Pierucci*) un Eiropas Padomes Datu aizsardzības komisārs Žans Filips Valters (*Jean-Philippe Walter*) pieņēma kopīgu paziņojumu, kurā valstis ir mudinātas stiprināt personas datu aizsardzību

327 Latvijā likums par Konvencijas 108 ratificēšanu pieņemts 2001. gada 5. aprīlī. Sk. Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi.

328 Sk. valstis, kas ir pievienojušās Konvencijai 108+: Council of Europe. Chart of signatures and ratifications of Treaty 223. Status as of 12/06/2021. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures?p_auth=iyy2ZbpX

329 Sk. Council of Europe. Recommendations, resolutions and guidelines. https://www.coe.int/en/web/cdcj/recommendations-resolutions-guidelines

330 Parliamentary Assembly of the Council of Europe. (2015). Resolution 2045. Mass surveillance. http://assembly.coe.int/nw/xml/xref/xref-xml2html-en.asp?fileid=21692&lang=en

331 Ibid., para 4.

332 Ibid., para 18, 19.

izlūkdienestu veiktās digitālās novērošanas kontekstā, pievienojoties Eiropas Padomes Konvencija 108+ un veicinot jaunu starptautisku tiesisku standartu izstrādi, lai šajā jomā nodrošinātu demokrātiskus un efektīvus aizsardzības pasākumus. Paziņojumā norādīts, ka valstīm starptautiskā līmenī ir jāvienojas par to, cik lielā mērā izlūkošanas dienestiem ir atļauts veikt novērošanu, kādos apstākļos un kādi aizsardzības pasākumi jāievēro.[333]

Jaunu tiesisko standartu izveide varētu balstīties uz kritērijiem, kurus jau ir izstrādājušas tiesas, tostarp EST.[334] Paziņojumā tiek vērsta uzmanība uz EST sprieduma "Schrems II" nozīmi. Tajā ir secināts, ka ES un ASV līgums jeb t. s. privātuma vairogs nenodrošina pietiekamu aizsardzības līmeni personas datiem, kas no ES pārsūtīti uz ASV, jo ASV valdības pārraudzītajā novērošanas programmā nav pietiekamu cilvēktiesību aizsardzības pasākumu saistībā ar piekļuvi datiem. Paziņojumā ir uzsvērts, ka šis spriedums ietekmē ne tikai datu nosūtīšanu no ES uz ASV, tas dod arī iespēju nostiprināt vispārējo datu aizsardzības sistēmu. Paziņojumā tiek arī atgādināts, ka Konvencijai 108+ ir būtiska nozīme, lai nodrošinātu stabilu juridiski saistošu vienošanos par privātuma un personas datu aizsardzību visā pasaulē, it īpaši attiecībā uz personas datu plūsmu pāri robežām. Tajā pašā laikā tiek arī norādīts – lai gan Konvencija 108+ paredz stabilu starptautisko tiesisko regulējumu personas datu aizsardzībai, tā pilnībā neatrisina dažādas problēmas, ko digitālajā laikmetā rada bezprecedenta novērošanas iespējas.

Eiropas Padome ir aktīvi iesaistījusies diskusijā un izstrādājusi dokumentus arī par jauno tehnoloģiju, īpaši mākslīgā intelekta sistēmu, ietekmi uz cilvēktiesībām. 2017. gadā Eiropas Padomes Parlamentārā asambleja publicēja Rekomendāciju par tehnoloģiju saplūšanu, mākslīgo intelektu un cilvēktiesībām.[335] Rekomendācijā norādīts, ka nanotehnoloģijas, biotehnoloģijas, informācijas tehnoloģijas un kognitīvo zinātņu saplūšana un ātrums, ar kādu jaunās tehnoloģijas tiek laistas tirgū, ietekmē ne tikai cilvēktiesības un veidu, kā tās var tikt īstenotas, bet arī pamatkoncepciju par to, kas raksturo cilvēku. Jauno tehnoloģiju un to izmantošanas veidu pieaugums izjauc robežas starp cilvēku un mašīnu, starp

333 Council of Europe. (2020). Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. https://rm.coe.int/covid19-joint-statement/16809e09f4

334 Council of Europe. (2020). Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services. Joint statement by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb

335 Parliamentary Assembly of the Council of Europe. (2017). Recommendation 2102. Technological convergence, artificial intelligence and human rights. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en

darbībām tiešsaistē un bezsaistē, starp fizisko un virtuālo pasauli, starp dabisko un mākslīgo. Lai aizsargātu cilvēka cieņu 21. gadsimtā, ir nepieciešamas jaunas pārvaldības formas, publiskas diskusijas un tiesiskie mehānismi. Rekomendācijā Eiropas Padome tiek aicināta attiecīgajām institūcijām uzdot izvērtēt, kā tehnoloģiju saplūšana un tās sociālās un ētiskās sekas, kas saistītas ar ģenētiku un genomiku, neirozinātni un lielo datu jomu, izaicina dažādas cilvēktiesību dimensijas.

Konvencijas 108 Konsultatīvā komiteja ir izstrādājusi vairākus dokumentus, kuros analizēti izaicinājumi, ko jaunās tehnoloģijas, īpaši mākslīgais intelekts, rada cilvēktiesībām. 2017. gadā tika pieņemtas Vadlīnijas par personu aizsardzību attiecībā uz personas datu apstrādi lielo datu pasaulē.[336] 2019. gadā tā publicēja Alesandro Mantelero (*Alessandro Mantelero*) izstrādāto ziņojumu "Mākslīgais intelekts un datu aizsardzība: izaicinājumi un iespējamie aizsardzības līdzekļi".[337] 2019. gadā Konvencijas 108 Konsultatīvā komiteja publicēja Vadlīnijas par mākslīgo intelektu un datu aizsardzību.[338]

2019. gadā Eiropas Padomes Ministru komiteja pieņēma Deklarāciju par algoritmisko procesu manipulācijas iespējām, kas brīdina, ka algoritmiskos procesus var izmantot, lai manipulētu ar sociālo un politisko uzvedību. Deklarācijā tiek vērsta uzmanība uz "draudiem demokrātiskai sabiedrībai", ko rada "mašīnmācīšanās rīku spēja ietekmēt emocijas un domas, kā arī valstis tiek mudinātas šos draudus novērst".[339]

2020. gadā Eiropas Padomes Ministru komiteja pieņēma Rekomendāciju dalībvalstīm par algoritmisko sistēmu ietekmi uz cilvēktiesībām.[340] Tā uzsver, ka cilvēka cieņas aizsardzība un cilvēktiesību un pamatbrīvību aizsardzība, īpaši tiesības uz personas datu aizsardzību, ir būtiskas, izstrādājot un ieviešot mākslīgā intelekta sistēmas, kas var ietekmēt indivīdus un sabiedrību, īpaši, ja šīs sistēmas tiek izmantotas lēmumu pieņemšanas procesos. Vadlīnijās ir norādīts, ka mākslīgā intelekta izstrādei, kas ietver personas datu apstrādi, ir jābalstās uz Konvencijā 108+ noteiktajiem principiem. Šie galvenie principi ir likumība, taisnīgums,

336 Council of Europe (2017), Consultative Committee of the Convention for the Protection .. (T-PD).

337 Council of Europe. (2019). Report on Artificial Intelligence and Data Protection: Challenges and Possible Remedies. https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6

338 Council of Europe. (2019). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). Guidelines of Artificial Intelligence and Data Protection. https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

339 Council of Europe (2019), Declaration by the Committee of Ministers on the manipulative capabilities ..

340 Council of Europe (2020), Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States ..

mērķa precizēšana, datu apstrādes samērīgums, integrēta datu aizsardzība (*privacy by design* – angļu val.) un datu aizsardzība pēc noklusējuma (*privacy by default* – angļu val.), atbildība un atbilstības pierādīšana, pārredzamība, datu drošība un risku pārvaldība. Rekomendācijā tiek uzsvērts, ka uz iespējamām datu apstrādes sekām ir jāskatās plašāk – jāņem vērā ne tikai cilvēktiesības un pamatbrīvības, bet arī ietekme uz demokrātiju un sociālās un ētiskās vērtības.

Eiropas Padomes Ministru komitejas izveidotā CAHAI 2020. gada decembrī publicēja priekšizpētes pētījumu, kurā ir piedāvāti vairāki iespējamie varianti Eiropas tiesiskajam regulējumam.[341] Viena no iespējām būtu spēkā esošo juridiski saistošo tiesisko instrumentu modernizācija, piemēram, pieņemot ECTK papildu protokolu, modernizējot Budapeštas konvenciju par kibernoziegumiem[342] vai Konvenciju 108+. Otra iespēja ir pieņemt jaunu saistošu tiesisko instrumentu, piemēram, konvenciju vai pamatkonvenciju. Pamatkonvencija paredzētu, ka valstis savstarpēji vienotos par tiesiskā regulējuma darbības jomu un procedūru, kas jāievēro, lai piedāvātu efektīvus aizsardzības pasākumus mākslīgā intelekta sistēmām, pamatojoties uz Eiropas Padomes standartiem. Trešā iespēja būtu pieņemt nesaistošus tiesiskus instrumentus. CAHAI vērš uzmanību, ka tiesiskais regulējums, visticamāk, būtu jāveido, apvienojot gan saistošus, gan nesaistošus juridiskus instrumentus, kas cits citu papildinātu. Saistošs horizontāls instruments, t. i., konvencija vai pamatkonvencija, varētu konsolidēt vispārīgus principus, lai novērstu riskus, kas raksturīgi mākslīgā intelekta videi, un iekļautu konkrētākus noteikumus, lai aizsargātu cilvēka cieņu, novērstu kaitējumu un veicinātu cilvēktiesības, demokrātiju, tiesiskumu, kā arī nodrošinātu citas tiesības, ētikas principus un pienākumus – cilvēka brīvību un autonomiju, nediskrimināciju, dzimumu līdztiesību, taisnīgumu un daudzveidību, pārredzamību un izskaidrojamību, datu aizsardzību, tiesības uz privātumu un atbildību. Tas varētu veidot pamatu attiecīgajiem valstu tiesību aktiem šajā jomā un veicināt paraugpraksi mākslīgā intelekta regulējuma izstrādē. Šo instrumentu, kas varētu ietvert atbilstošus pēcpārbaudes mehānismus un procesus, varētu papildināt gan juridiski saistoši, gan nesaistoši Eiropas Padomes instrumenti konkrētās nozarēs, un tie varētu paredzēt turpmākus nozarei specifiskus principus un sīki izstrādātas prasības par to, kā risināt mākslīgā intelekta nozares problēmas.

2021. gada 21. janvārī Eiropas Padome publicēja Vadlīnijas par sejas atpazīšanu, un šajā dokumentā valstis tiek mudinātas izstrādāt un pieņemt speciālus noteikumus, kas regulētu tiesībaizsardzības nolūkos veiktu biometrisko datu

341 Council of Europe, CAHAI (2020), Feasibility Study.

342 Konvencija par kibernoziegumiem. Pieņemta 23.11.2001. (EP, Latvijā spēkā no 01.06.2007.). *Latvijas Vēstnesis,* 26.10.2001., Nr. 171.

apstrādi, izmantojot sejas atpazīšanas tehnoloģijas, kā arī aizliegtu konkrētus šīs tehnoloģijas izmantošanas gadījumus.[343]

Eiropas Padome nebūt nav vienīgā organizācija, kas aktīvi meklē veidus, kā regulēt mākslīgo intelektu. Arī citas organizācijas, kas aplūkotas turpinājumā, aktīvi darbojas, lai ietekmētu datu aizsardzības tiesību, kā arī jauno tehnoloģiju regulējuma attīstību.

4.1.2. OECD

Līdzās Eiropas Padomei, kas datu aizsardzību pamatā skata no cilvēktiesību aizsardzības skatpunkta, Ekonomiskās sadarbības un attīstības organizācija (*Organisation for Economic Cooperation and Development*, OECD – angļu val.) ir izstrādājusi nozīmīgu instrumentu, kas ietekmējis mūsdienu datu aizsardzības tiesību izveidi, bet iezīmē ekonomisko pieeju datu aizsardzībai, – Vadlīnijas par privātuma aizsardzību un pārrobežu personas datu plūsmu.[344]

OECD ir 1961. gadā dibināta starpvaldību organizācija, kuras uzdevums ir veicināt demokrātiju un tirgus ekonomikas principu ievērošanu, kā arī sekmēt valstu ilgtspējīgas tautsaimniecības attīstību globalizācijas kontekstā. Tā apvieno 38 attīstītākās pasaules valstis, sākot no Ziemeļamerikas un Dienvidamerikas līdz Eiropai un Āzijas un Klusā okeāna reģionam, tai skaitā ES dalībvalstis. Latvija par OECD dalībvalsti kļuva 2016. gadā.

OECD pirmām kārtām ir ekonomikas organizācija, un, kā jau liecina tās nosaukums, tās darbība galvenokārt ir saistīta ar sadarbības veicināšanu starp valstīm, lai veicinātu ekonomisko attīstību, finansiālo stabilitāti, dzīves līmeņa paaugstināšanu un starptautiskās tirdzniecības attīstību. Tā koordinē nacionālo un starptautisko politiku izstrādi, tostarp izstrādā vadlīnijas, standartus un starptautiskos tiesību instrumentus galvenokārt ar ekonomiku saistītos jautājumos.

Lai gan OECD darbība atšķirībā no Eiropas Padomes nav primāri saistīta ar cilvēktiesību aizsardzību, tā aktīvi iesaistās datu aizsardzības jautājumu attīstībā. OECD darbs pie privātuma un datu aizsardzības jautājumiem sākās 1969. gadā, kad tika nozīmēta ekspertu grupa, lai analizētu dažādus privātuma jautājumus, tostarp saistībā ar digitālo informāciju, valsts pārvaldi un pārrobežu datu nodošanu. 1979. gadā OECD sarīkoja simpoziju par pārrobežu datu plūsmas un privātuma aizsardzības jautājumiem, tajā piedalījās pārstāvji no dalībvalstīm, privātā sektora un starptautiskām organizācijām. Francijas pārstāvis Luijs Žoinē (*Louis*

343 Council of Europe (2021), .. Convention 108.

344 OECD. (1980). Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Joinet), kurš vēlāk piedalījās vadlīniju izstrādē, uzsvēra ekonomisko vērtību un nacionālo interešu sadursmi, ko rada pārrobežu datu plūsma: "Informācija ir vara, un ekonomiskā informācija ir ekonomiska vara. Informācijai ir ekonomiska vērtība, un spēja uzglabāt un apstrādāt noteikta veida datus vienai valstij var dot politiskas un tehnoloģiskas priekšrocības salīdzinājumā ar citām valstīm."[345]

1978. gadā OECD izveidoja jaunu darba grupu pārrobežu datu barjeru un privātuma aizsardzības jautājumos un tai uzticēja izstrādāt vadlīniju projektu. Darba grupas izstrādātās Vadlīnijas par privātuma aizsardzību un pārrobežu personas datu plūsmu 1980. gadā pieņēma OECD Padome. Vadlīniju mērķis bija saskaņot valstu tiesību aktus, uzsvaru liekot uz šķēršļu novēršanu brīvai datu plūsmai. Vadlīnijās uzsvērts, ka ir jānodrošina, lai privātuma aizsardzības intereses tiktu līdzsvarotas ar personu datu brīvu pārrobežu plūsmu interesēm un nav pieļaujama tādu šķēršļu radīšana personas datu plūsmām, kuri tiek pamatoti ar privātās dzīves un indivīdu brīvību aizsardzību, bet patiesībā ir pieņemti, lai sasniegtu cita veida ierobežojošus mērķus, kuri netiek atklāti paziņoti.[346]

OECD vadlīnijas tika izstrādātas ciešā sadarbībā ar Eiropas Kopienu un Eiropas Padomi, tādējādi nodrošinot to atbilstību datu aizsardzības principiem, kas tajā pašā laikā tika izstrādāti Eiropā. Vadlīnijas tika pārskatītas 2013. gadā. Lai gan vadlīnijas nav juridiski saistošas, tomēr tām bija būtiska nozīme datu aizsardzības tiesību harmonizācijā visā pasaulē.

OECD aktīvi darbojas arī mākslīgā intelekta politikas jomā. 2019. gadā OECD dalībvalstis pieņēma "Padomes Rekomendāciju par mākslīgo intelektu", ko parakstīja 42 valstu pārstāvji un kas nosaka pirmos starptautiskos standartus, par kuriem valdības ir vienojušās, lai izveidotu atbildīgu un uzticamu mākslīgo intelektu.[347] Rekomendācijas mērķis ir sekmēt inovācijas un veicināt uzticamu un atbildīgu mākslīgā intelekta pārvaldību, vienlaikus nodrošinot cilvēktiesību un demokrātisko vērtību ievērošanu.

Rekomendācijā ir noteikti pieci uz vērtībām balstīti principi uzticama mākslīgā intelekta atbildīgai pārvaldībai. Pirmais princips paredz, ka mākslīgajam intelektam vajadzētu dot labumu cilvēkiem un planētai, veicinot iekļaujošu izaugsmi, ilgtspējīgu attīstību un labklājību. Otrais princips – uz cilvēku vērstas vērtības un taisnīgums – paredz, ka mākslīgā intelekta sistēmas būtu jāveido tā, lai tiktu ievērots tiesiskums, cilvēktiesības, demokrātiskās vērtības. Tās ietver brīvību, cieņu un autonomiju, privātumu un datu aizsardzību, nediskrimināciju un vienlīdzību, daudzveidību, taisnīgumu, sociālo taisnīgumu un starptautiski

345 OECD. (2013). The OECD Privacy Framework. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

346 OECD (1980), Recommendation of the Council concerning Guidelines Governing ..

347 OECD (2019), Recommendation of the Council on Artificial Intelligence.

atzītas darba tiesības. Šajā nolūkā būtu jāievieš atbilstoši mehānismi un aizsardzības pasākumi, piemēram, vajadzības gadījumā nodrošinot cilvēka iejaukšanos. Trešais princips paredz, ka ir jābūt pārredzamībai un atbildīgai informācijas atklātībai par mākslīgā intelekta sistēmām, lai nodrošinātu, ka cilvēki saprot sistēmas, ir informēti par to izmantošanu, kā arī tie, kurus ietekmē mākslīgā intelekta sistēmu rezultāti, varētu tos saprast un apstrīdēt. Ceturtais princips paredz, ka mākslīgā intelekta sistēmām visā to dzīves ciklā jādarbojas stabili un droši, iespējamie riski pastāvīgi jānovērtē un jāpārvalda. Pēdējais, piektais, princips nosaka, ka organizācijām un privātpersonām, kas izstrādā, izvērtē vai izmanto mākslīgā intelekta sistēmas, jābūt atbildīgām par to pareizu darbību saskaņā ar iepriekš minētajiem principiem. Rekomendācija sniedz arī piecus vispārējus ieteikumus dalībvalstīm, ko ieviest valstu politikā un starptautiskajā sadarbībā atbildīga mākslīgā intelekta nodrošināšanai, tai skaitā mudinot investēt mākslīgā intelekta pētniecībā un attīstībā un izveidot mākslīgā intelekta normatīvo regulējumu.

2020. gadā OECD izveidoja Mākslīgā intelekta politikas observatoriju jeb novērošanas centru "OECD.AI"[348], kas ir iekļaujošs sabiedriskās politikas centrs mākslīgā intelekta jomā. Tā mērķis ir palīdzēt valstīm izveidot, attīstīt un uzraudzīt uzticamu un atbildīgu mākslīgā intelekta sistēmu attīstību sabiedrības labā. "OECD.AI" ir tiešsaistes platforma, kur mākslīgā intelekta dalībnieki var dalīties ar informāciju un sadarboties, veidojot ar mākslīgo intelektu saistītu politiku. 2020. gadā tika arī nodibināta Globālā mākslīgā intelekta partnerība[349], kuras sekretariāts ir OECD. Tās mērķis ir pārvarēt plaisu starp teoriju un praksi mākslīgā intelekta politikas jomā un nodrošināt mākslīgā intelekta atbildīgu izmantošanu.

4.1.3. ANO, UNESCO un citi globālie standarti

Tiesības uz privātumu ir noteiktas starptautiskos cilvēktiesību aizsardzības līgumos – Vispārējās cilvēktiesību deklarācijas 12. pantā, SPPPT 17. pantā u. c. Savukārt tiesības uz datu aizsardzību vismaz pagaidām nav atzītas par universālām cilvēktiesībām. Globālā līmenī nav panākta vienošanās par juridiski saistošiem minimālajiem datu aizsardzības standartiem, lai gan šādi priekšlikumi ir bijuši. Vienoties par kopīgiem standartiem traucē būtiski atšķirīga pieeja dažādās tiesību

348 Sk. OECD. AI Policy Observatory. https://oecd.ai

349 Globālās mākslīgā intelekta partnerības dibinātāji ir ES, Austrālija, Kanāda, Francija, Vācija, Indija, Itālija, Japāna, Koreja, Meksika, Jaunzēlande, Singapūra, Slovēnija, Lielbritānija un ASV, un tā apvieno nozares, valdības, pilsoniskās sabiedrības un akadēmisko aprindu ekspertus, lai veiktu mākslīgā intelekta pētījumus. Sk. The Global Partnership on Artificial Intelligence. https://gpai.ai

sistēmās, īpaši starp valstīm, kurās tās vēsturiski ir attīstījušās kā cilvēktiesības, un valstīm, kur datu aizsardzībai ir vairāk ekonomisks pamats.[350]

Tajā pašā laikā ANO ir ļoti nozīmīga loma privātuma un datu aizsardzības veicināšanā. 1990. gadā ANO Ģenerālā asambleja publicēja Vadlīnijas datorizētu personas datu failu regulēšanai. Tās paredz principus, kuri kā minimālās prasības valstīm būtu jāietver nacionālajā likumdošanā, piemēram, likumīgums, taisnīgums, precizitāte, noteikts mērķis, ieinteresēto personu piekļuve, nediskriminācijas princips. Kā atsevišķs princips ir paredzēta arī spēja izdarīt izņēmumus no iepriekš minētajiem principiem, ja tie ir nepieciešami, lai aizsargātu valsts drošību, sabiedrisko kārtību un sabiedrības veselību, ja šāda atkāpšanās ir skaidri noteikta likumā vai līdzvērtīgā regulējumā, kas pieņemts saskaņā ar nacionālo tiesību sistēmu, kurā paredzētas skaidras robežas un atbilstoši aizsardzības pasākumi.

Vadlīnijas ietver arī drošības principu, kas nosaka, ka būtu jāveic atbilstoši pasākumi, lai aizsargātu datus no dažāda veida riskiem, piemēram, nejaušas nozaudēšanas vai iznīcināšanas, neatļautas piekļuves, krāpnieciskas datu ļaunprātīgas izmantošanas vai datorvīrusu piesārņojuma. Tās paredz, ka katras valsts likumi nosaka iestādi, kas saskaņā ar tās nacionālo tiesību sistēmu ir atbildīga par iepriekš izklāstīto principu ievērošanas uzraudzību, kā arī paredz pienākumu nodrošināt brīvu datu plūsmu.[351]

ANO ir arī plaši vērsusi uzmanību uz masveida novērošanas radīto apdraudējumu cilvēktiesībām. Reaģējot uz E. Snoudena atklājumiem, 2013. gadā ANO Ģenerālā asambleja pieņēma rezolūciju 68/167 "Tiesības uz privātumu digitālajā laikmetā"[352], kurā pauda bažas par komunikāciju uzraudzības un pārtveršanas, kā arī personas datu vākšanas, it īpaši, ja to veic masveidā, negatīvo ietekmi uz cilvēktiesībām, un mudināja valstis izveidot vai uzturēt neatkarīgus un efektīvus uzraudzības mehānismus, kas var nodrošināt novērošanas darbību pārredzamību un atbildību.

Pēc Ģenerālās asamblejas pieprasījuma 2014. gadā ANO Augstā cilvēktiesību komisāra birojs publicēja ziņojumu "Tiesības uz privāto dzīvi digitālajā laikmetā", kurā ir aplūkota tiesību uz privātumu aizsardzība un veicināšana novērošanas kontekstā, kā arī digitālo komunikāciju pārtveršana un personas datu vākšana, tostarp masveidā.[353] Ziņojumā ir uzsvērts, ka masveida novērošana līdzās tiesībām uz privātumu var ietekmēt arī citas ar tām cieši saistītas tiesības – tiesības uz

350 Lloyd (2020), Information Technology Law, pp. 33, 34.

351 UN General Assembly. (1990). Guidelines for the Regulation of Computerized Personal Data Files. https://www.refworld.org/docid/3ddcafaac.html

352 UN General Assembly. (2013). Resolution 68/167. The right to privacy in the digital age. https://digitallibrary.un.org/record/764407/?ln=en

353 OHCHR (2014), The right to privacy in the digital age.

uzskatu un vārda brīvību, tiesības meklēt, saņemt un izplatīt informāciju, mierīgas pulcēšanās un biedrošanās brīvību un tiesības uz ģimenes dzīvi.

Ziņojumā ir norādīts, ka mērķtiecīga digitālās komunikācijas uzraudzība var būt nepieciešams un efektīvs pasākums izlūkdienestiem un tiesībaizsardzības iestādēm, ja tā tiek veikta saskaņā ar starptautiskajiem un nacionālajiem tiesību aktiem. Valdībai ir jāpierāda, ka iejaukšanās ir nepieciešama un proporcionāla adresētajam specifiskajam riskam. Tādējādi masveida vai "liela apjoma" novērošanas programmas var uzskatīt par patvaļīgām, pat ja tām ir leģitīms mērķis un ja tās ir paredzētas tiesiskajā regulējumā. Ziņojumā minēts: nebūtu pieļaujams, ka "pasākumi ir vērsti uz adatu meklēšanu siena kaudzē"; par atbilstošu ir uzskatāms tāds pasākums, kas ņem vērā ietekmi uz "siena kaudzi" salīdzinājumā ar apdraudēto kaitējumu; proti, vai pasākums ir nepieciešams un samērīgs. Līdzās valsts iestāžu atbildībai turpmākajos ziņojumos arvien vairāk uzmanība pievērsta arī privātā sektora atbildībai par cilvēktiesību ievērošanu un aicinājums uzņēmumiem informēt lietotājus par personas datu vākšanu, izmantošanu, koplietošanu un saglabāšanu, kā arī izveidot pārredzamu datu apstrādes politiku.[354]

2015. gadā ANO Cilvēktiesību padome iecēla IT ekspertu profesoru Džozefu Kanataci (*Joseph Cannataci*) par pirmo īpašo referentu jautājumos par tiesībām uz privātumu. Referenta īpašie uzdevumi ietver informācijas vākšanu par valstu praksi un pieredzi saistībā ar privātumu un jauno tehnoloģiju izaicinājumiem, paraugprakses apmaiņu un veicināšanu, kā arī iespējamo šķēršļu noteikšanu. Viņš ir pievērsis pastiprinātu uzmanību digitālo komunikāciju pārtveršanai un personas datu vākšanai, īpaši masveida novērošanas kontekstā. 2017. gada īpašā referenta ikgadējais ziņojums bija veltīts valsts novērošanas darbībām no nacionālā un starptautiskā skatpunkta un sniedza sākotnējos ieteikumus pasākumu aizsardzības garantijām, uzsverot nepieciešamību nodrošināt pārredzamību un pārskatatbildību.[355] Arī turpmākos ikgadējos ziņojumos pastiprināta uzmanība ir vērsta uz cilvēktiesību riskiem, ko rada valstu masveida novērošanas pasākumi.[356]

354 Sk. OHCHR. (2018). The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. https://digitallibrary.un.org/record/777869#record-files-collapse-header

355 UN Special Rapporteur on the right to privacy. (2017). Report of the Special Rapporteur on the right to privacy. https://digitallibrary.un.org/record/3845912

356 UN Special Rapporteur on the right to privacy. (2018). Report of the Special Rapporteur on the right to privacy. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/324/47/PDF/G1832447.pdf?OpenElement; UN Special Rapporteur on the right to privacy. (2019). Right to privacy. Report of the Special Rapporteur on the right to privacy. https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08;%20https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx

ANO īpašā referenta jautājumos par tiesībām uz privātumu 2020. gada ziņojumā atsevišķa nodaļa ir veltīta drošībai un novērošanai, kurā norādīti ieteikumi valstīm un nevalstiskiem dalībniekiem. Tiem ir jāaizsargā digitālo komunikāciju privātums un visu personu tiesības uz privātumu neatkarīgi no viņu dzimuma, veicinot tādus rīkus kā šifrēšana. Tiem vajadzētu nodrošināt, ka tiesību uz privātumu ierobežojumi – tostarp masveida vai mērķtiecīga novērošana, personas datu pieprasījumu vai šifrēšanas, pseidonimizēšanas un anonimizēšanas rīku izmantošanas ierobežojumi – ir balstīti uz katru gadījumu atsevišķi; nediskriminē pēc dzimuma vai citiem faktoriem; ir saprātīgi, nepieciešami un samērīgi, kā to paredz likums; tiem ir leģitīms mērķis, un tos apstiprina tikai tiesa.[357]

ANO aktīvi iesaistās arī starptautiskajās diskusijās par mākslīgā intelekta regulējumu. 2018. gadā Starptautiskā telekomunikāciju savienība ar vairāk nekā 25 ANO aģentūrām Ženēvā rīkoja "AI for Good" samitu, kurā ANO ģenerālsekretārs Antoniu Gutērrešs (*António Guterres*) atzina, ka, ņemot vērā mākslīgā intelekta straujo attīstību, ir jārada jaunas platformas, lai novērstu tā radītos riskus, un uzsvēra vēlmi, lai ANO būtu platforma, kurā dažādas grupas sanāktu kopā, lai apspriestu un vienotos par protokoliem un citiem mehānismiem, kā nodrošināt, ka kibertelpa, internets un mākslīgais intelekts būtu "labā spēks" (*force for good* – angļu val.).[358] 2018. gadā ANO ģenerālsekretārs pieņēma Jauno tehnoloģiju stratēģiju[359], kurā uzsvērts, ka viens no pamatprincipiem ir, ka jaunajām tehnoloģijām jābalstās uz globālām vērtībām, kas noteiktas ANO Hartā[360] un Vispārējā cilvēktiesību deklarācijā.

2020. gada septembrī ANO īpašais referents jautājumos par tiesībām uz privātumu publicēja projektu Datu privātuma vadlīnijām mākslīgā intelekta izstrādei un darbībai. Vadlīnijas paredzēts piemērot mākslīgā intelekta risinājumiem, kas veic datu apstrādi, visos sektoros, tostarp publiskajā un privātajā sektorā. Vadlīnijas nosaka, ka mākslīgā intelekta risinājumu plānošanā un ieviešanā kā obligāti apsverami šādi septiņi galvenie principi: 1) jurisdikcija; 2) likumīgs pamats un

357 UN Special Rapporteur on the right to privacy. (2020). Report of the Special Rapporteur on the right to privacy. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/071/66/PDF/G2007166.pdf?OpenElement

358 UN News. (5 November, 2018). 'Warp speed' technology must be 'force for good' UN chief tells web leaders. https://news.un.org/en/story/2018/11/1024982

359 UN. (2018). UN Secretary-General's Strategy on new technologies. https://www.un.org/en/newtechnologies/images/pdf/SGs-Strategy-on-New-Technologies.pdf

360 Apvienoto Nāciju Organizācijas Statūti. Pieņemti 26.06.1945. (Latvijā spēkā no 17.09.1991.). *Latvijas Vēstnesis*, 29.01.2018., Nr. 20.

nolūka ierobežojums; 3) atbildība; 4) kontrole; 5) pārredzamība un izskaidrojamība; 6) datu subjekta tiesības; 7) drošības pasākumi.[361]

Vadlīniju projektā ir paredzētas būtiskas datu aizsardzības prasības. Likumīga pamata prasība paredz, ka mākslīgā intelekta risinājumiem, ja tie attiecas uz personas datiem, ir jābūt tiesiskam pamatam, jo personas datu apstrāde vienmēr ietekmē datu subjekta tiesības. Saskaņā ar pārredzamības principu mākslīgā intelekta risinājumiem ir jābūt pārredzamiem sabiedrībai un datu subjektiem. Vadlīnijās ir noteiktas datu subjektu tiesības, tostarp: tiesības uz informāciju; tiesības uz samērīgu piekļuvi saviem datiem, kas ietver izsmeļošu rakstisku informāciju par personas datiem un to, kā tie tiek izmantoti un apstrādāti, kā arī sekām un veidiem, kā mākslīgā intelekta sistēmu rezultāti var ietekmēt datu subjekta stāvokli un individuālās tiesības; tiesības pieprasīt cilvēka lēmumu, ja ir pamatotas šaubas par to, vai mākslīgā intelekta risinājuma piedāvātais vai pieņemtais lēmums nav pareizs; tiesības labot datus, ja tie ir nepareizi; tiesības iesniegt sūdzību, ja ir pamatots iemesls.

Daudzas ANO aģentūras, iestādes un pētniecības institūti aktīvi iesaistās atbildīga mākslīgā intelekta veicināšanā. 2019. gadā tika publicēts ANO Starpreģionālās noziedzības un tieslietu pētniecības institūta (UNICRI) un Starptautiskās Kriminālpolicijas organizācijas (Interpol) kopīgs ziņojums par mākslīgo intelektu un robotiku tiesībaizsardzības iestādēs, kurā norādīts, ka mākslīgais intelekts un robotika ievērojami veicinās tiesībaizsardzības iestāžu novērošanas iespējas un tāpēc būs jārisina ar šīm tehnoloģijām saistītās privātuma problēmas.[362]

Konkrētāk uz novērošanas tehnoloģiju riskiem un nepieciešamo regulējumu uzmanību vērsusi ANO Augstā cilvēktiesību komisāra biroja Rasu diskriminācijas izskaušanas komiteja, kas 2020. gadā pieņēma Vispārējo rekomendāciju Nr. 36 par rasu profilēšanas novēršanu un apkarošanu, ko veic tiesībaizsardzības iestāžu amatpersonas.[363] Rekomendācijas 53. punktā ir atzīts, ka sejas atpazīšanas un novērošanas tehnoloģiju aizvien plašāka izmantošana, lai izsekotu un kontrolētu cilvēkus pēc konkrētām demogrāfiskām pazīmēm, rada bažas par daudzām cilvēktiesībām, tostarp tiesībām uz privātumu, mierīgas pulcēšanās un biedrošanās brīvību, vārda brīvību un pārvietošanās brīvību. Šīs tehnoloģijas ir izstrādātas, lai automātiski identificētu personas, pamatojoties uz viņu sejas ģeometriju, kas

361 UN Special Rapporteur on the right to privacy. (2020). Draft for Consultations. Data Privacy Guidelines for the development and operation of Artificial Intelligence solutions. https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2020_Sept_draft_data_Privacy_guidelines.pdf

362 UNICRI & INTERPOL. (2019). Artificial Intelligence and Robotics for Law Enforcement. https://unicri.it/artificial-intelligence-and-robotics-law-enforcement

363 UN Committee on the Elimination of Racial Discrimination. (2020). General recommendation No. 36. Preventing and Combating Racial Profiling by Law Enforcement Officials. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/349/50/PDF/G2034950.pdf?OpenElement

ļauj potenciāli profilēt tās, balstoties uz diskriminējošiem pamatiem, piemēram, rasi, ādas krāsu, nacionālo vai etnisko izcelsmi vai dzimumu. Turklāt ir pierādīts, ka sejas atpazīšanas tehnoloģijas precizitāte var atšķirties atkarībā no novērtēto personu ādas krāsas, etniskās piederības vai dzimuma, un tas var izraisīt diskrimināciju. Tālāk Rekomendācijas 59. punktā ir norādīts, ka, pirms tiek izmantotas sejas atpazīšanas tehnoloģijas, valstīm ir rūpīgi jāizvērtē to ietekme uz cilvēktiesībām, jo tās var izraisīt kļūdainu identifikāciju. Pirms to ieviešanas valstīm būtu jāapsver izmēģinājuma periods, kura laikā šo tehnoloģiju darbību uzraudzītu neatkarīgas institūcijas un šo tehnoloģiju precizitāte tiktu pārbaudīta, iekļaujot personas, kas pārstāv dažādas iedzīvotāju grupas, lai samazinātu iespēju, ka personas tiek nepareizi identificētas un profilētas atkarībā no ādas krāsas.

UNESCO ir pieņēmusi Rekomendāciju par mākslīgā intelekta ētiku.[364] Tā ir pirmā globālā vienošanās, kas nosaka standartus mākslīgā intelekta ētikas jomā. UNESCO ģenerāldirektore Odrē Azulē (*Audrey Azoulay*) 2020. gada martā nozīmēja 24 ekspertus, izveidojot starptautisko *ad hoc* ekspertu grupu (AHEG), kas 2020. gadā sagatavoja pirmo rekomendācijas projektu.[365] 2020. gada vasarā notika plašs tā apspriešanas process. Tā paša gada septembrī Rekomendācijas projekts tika nodots dalībvalstīm. 2021. gadā aprīlī un jūnijā tas tika izskatīts UNESCO Starpvaldību komitejā. 2021. gada 24. novembrī UNESCO Ģenerālās konferences 41. sesijā 193 valstis vienojās par Rekomendācijas par mākslīgā intelekta ētiku pieņemšanu.

Rekomendācijas mērķis ir nodrošināt, lai mākslīgā intelekta sistēmas darbotos cilvēces, personu, sabiedrības, kā arī vides un ekosistēmu labā, kā arī novērst to radīto kaitējumu. Rekomendācijas mērķis ir arī veicināt mākslīgā intelekta sistēmu miermīlīgu izmantošanu (5. punkts). Rekomendācija veicina cilvēktiesību, cilvēka cieņas, dzimumu līdztiesības, tiesiskuma un demokrātijas vērtību ievērošanu. Lai gan tajā īpaša uzmanība pievērsta mākslīgā intelekta sistēmu ietekmei uz UNESCO galvenajām darbības jomām – izglītību, zinātni, kultūru, komunikāciju un informāciju –, tajā pašā laikā tās noteikumi ir vispārīgi un attiecināmi uz ikvienu mākslīgā intelekta jomu.

Rekomendācija ne tikai nosaka vērtības un principus, bet arī sniedz konkrētus ieteikumus un paredz praktiskus to īstenošanas mehānismus. Valstis tiek aicinātas tos ņemt vērā, izstrādājot savus tiesību aktus, politikas dokumentus vai citus instrumentus attiecībā uz mākslīgo intelektu saskaņā ar starptautiskajām tiesībām. Rekomendācija balstās uz četrām vērtībām. Tās ir:

364 UNESCO (2021), Recommendation on the Ethics of Artificial Intelligence.

365 UNESCO. (2020). Composition of the Ad Hoc Expert Group (AHEG) for the Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000372991.

1) cilvēktiesību, pamatbrīvību un cilvēka cieņas ievērošana, aizsardzība un veicināšana;
2) vides un ekosistēmas aizsardzības veicināšana;
3) daudzveidības un iekļaušanas nodrošināšana;
4) dzīvošana mierīgā, taisnīgā un savstarpēji saistītā sabiedrībā.

Ja vērtības motivē, sniedz ideālus un iedvesmo uz rīcību, tad principi konkrētāk definē šīs vērtības, lai tās varētu vieglāk ietvert konkrētos politikas ieteikumos. Rekomendācijā ir noteikti desmit principi: 1) proporcionalitāte un nekaitēšana; 2) drošība; 3) taisnīgums un nediskriminācija; 4) ilgtspējība; 5) tiesības uz privātumu un datu aizsardzība; 6) cilvēka pārraudzība; 7) pārredzamība un izskaidrojamība; 8) atbildība; 9) apzināšanās un zināšanas; 10) daudzpusīga un adaptīva pārvaldība un sadarbība.

Pirmais princips – proporcionalitāte un nekaitēšana – paredz, ka izvēle izmantot mākslīgā intelekta sistēmas un to, kuru mākslīgā intelekta metodi izmantot, būtu jāpamato šādi:

a) izvēlētajai mākslīgā intelekta metodei jābūt piemērotai un samērīgai, lai sasniegtu noteiktu leģitīmu mērķi;
b) izvēlētā mākslīgā intelekta metode nedrīkst pārkāpt rekomendācijā ietvertās pamatvērtības, it īpaši tās izmantošana nedrīkst pārkāpt cilvēktiesības;
c) mākslīgā intelekta metodei jāatbilst kontekstam un jābūt balstītai uz stingriem zinātniskiem pamatiem.

Minētais princips nosaka arī mākslīgā intelekta sistēmu izmantošanas sarkanās līnijas. Tas nosaka, ka gadījumos, kad lēmumiem var būt neatgriezeniska vai grūti maināma ietekme vai tie var ietvert lēmumus par dzīvību un nāvi, galīgais lēmums ir jāpieņem cilvēkam. Tālāk tas paredz, ka mākslīgā intelekta sistēmas nedrīkst izmantot sociālās vērtēšanas vai masveida novērošanas nolūkos (25. punkts).

Rekomendācijā galvenā uzmanība ir veltīta politikas ieteikumiem. Viens no būtiskākajiem ieteikumiem ir, lai dalībvalstis ieviestu efektīvus mehānismus (ieskaitot politikas pamatnostādnes vai mehānismus) un nodrošinātu, ka visas ieinteresētās personas (piemēram, privātā sektora uzņēmumi, akadēmiskās un pētniecības iestādes), kā arī pilsoniskā sabiedrība tos ievēro, cita starpā palīdzot visām ieinteresētajām pusēm izstrādāt cilvēktiesību, tiesiskuma, demokrātijas un ētikas ietekmes novērtējumu un uzticamības pārbaudes rīkus. Šādas politikas vai mehānismu izstrādes procesā būtu jāiekļauj visas ieinteresētās puses, un tajā būtu jāņem vērā katras dalībvalsts apstākļi un prioritātes (49. punkts).

UNESCO var atbalstīt dalībvalstis politikas mehānismu izstrādē, kā arī uzraudzībā un novērtēšanā. Lai varētu efektīvi īstenot rekomendāciju, UNESCO apņemas izstrādāt gatavības novērtēšanas metodiku, lai palīdzētu dalībvalstīm noteikt savu statusu, ņemot vērā, ka valstis var atrasties dažādās stadijās

attiecībā uz gatavību ieviest Rekomendāciju dažādās jomās, piemēram, zinātniskajā, tehnoloģiju, ekonomiskajā, izglītības, juridiskajā, regulatīvajā, infrastruktūras, sabiedrības, kultūras jomā. Tāpat UNESCO apņemas atbalstīt dalībvalstis mākslīgā intelekta tehnoloģiju ētiskās ietekmes novērtēšanas metodikas izstrādē (49. punkts).

Rekomendācijā ietvertas vienpadsmit politikas plānošanas jomas: ētiskās ietekmes novērtējums; ētiska pārvaldība; datu politika; starptautiskā sadarbība un attīstība; vide un ekosistēmas; dzimumu līdztiesība; kultūra; izglītība un zinātne; komunikācija un informācija; ekonomika un darbaspēks; veselība un labklājība.

Viens no būtiskākajiem rekomendācijā paredzētajiem mehānismiem ir ētiskās ietekmes novērtējums. Dalībvalstis tiek aicinātas ieviest šādus novērtējumus, kas ļautu noteikt mākslīgā intelekta sistēmu ieguvumus, bažas un riskus, kā arī to novēršanas, mazināšanas un uzraudzības pasākumus. Ir nepieciešams novērtēt mākslīgā intelekta plašāku ietekmi uz cilvēktiesībām, darba tiesībām, vidi un ekosistēmu, kā arī ētisko un sociālo ietekmi (50. punkts).

Ētikas pārvaldības politikas joma paredz arī, ka dalībvalstīm būtu jānodrošina, lai mākslīgā intelekta sistēmu radītais kaitējums tiek izmeklēts un atlīdzināts, ieviešot spēcīgus aizsardzības mehānismus un pasākumus atbilstošas atlīdzības nodrošināšanai, lai garantētu cilvēktiesību un pamatbrīvību, un tiesiskuma ievērošanu digitālajā un fiziskajā pasaulē (55. punkts). Tiesiskajam regulējumam, kas attiecas uz mākslīgā intelekta sistēmām, jāatbilst starptautisko cilvēktiesību normām un jāveicina cilvēktiesības un pamatbrīvības visā mākslīgā intelekta sistēmas dzīves cikla laikā (61. punkts). Dalībvalstīm būtu jānosaka skaidras prasības mākslīgā intelekta sistēmas pārredzamībai un izskaidrojamībai, lai palīdzētu nodrošināt tās uzticamību (70. punkts).

Datu politikas joma paredz, ka dalībvalstīm ir jāievieš atbilstošas aizsardzības garantijas, lai atzītu un aizsargātu personas pamattiesības uz privātumu, tostarp pieņemot vai īstenojot tiesisko regulējumu, kas nodrošina atbilstošu aizsardzību un atbilst starptautiskajiem tiesību aktiem (72. punkts). Tām būtu arī jānodrošina, ka personas saglabā tiesības uz saviem personas datiem un tos aizsargā regulējums, kas it īpaši paredz pārredzamību, piemērotus drošības pasākumus sensitīvu datu apstrādei, augstāko datu drošības līmeni, efektīvas un jēgpilnas atbildības shēmas un mehānismus, pilnīgu datu subjektu tiesību izmantošanu (73. punkts).

Rekomendācija īpaši uzsver nepieciešamību izstrādāt atbilstošu tiesisko regulējumu, kā arī praktiskus to īstenošanas mehānismus. Lai gan ētikas standartiem ir būtiska loma risku novēršanā un samazināšanā, tajā pašā laikā ir svarīgi arī domāt, kā praksē īstenot šos ētikas principus. Kā atzīst Oksfordas Universitātes Interneta institūta pētnieks Brents Mitelštats (*Brent Mittelstadt*), bez būtiskām izmaiņām regulējumā principu ieviešana praksē paliks konkurējošs,

nevis sadarbības process.[366] Tiesiskās prasības ir svarīgs instruments, lai panāktu atbildību un nodrošinātu ētikas principu un sociālo vērtību īstenošanu praksē. Tāpēc ir pilnībā jāizvērtē esošā tiesiskā regulējuma atbilstība un nepilnības, un nepieciešamība pieņemt jaunu regulējumu.

Vienoties par globālu regulējumu traucē atšķirīgā izpratne par dažādiem principiem un to piemērošanu praksē, par to, kā samērojamas konkurējošas intereses, tostarp par privātuma un datu aizsardzības prasībām.[367] ES cilvēktiesību un datu aizsardzības augstie standarti bieži vien noder par paraugu citām valstīm un ietekmē arī mākslīgā intelekta starptautisko regulējumu.

4.2. Eiropas Savienība: no datu aizsardzības zelta standartiem līdz mākslīgā intelekta regulējumam

4.2.1. No ekonomiskās līdz cilvēktiesībās balstītai pieejai

ES sākotnēji tika veidota kā ekonomikas kopiena, nevis organizācija, kas aizsargā cilvēktiesības. Tajā pašā laikā pakāpeniski cilvēktiesību ievērošana ES ieguva arvien būtiskāku nozīmi, un mūsdienās ES ir kļuvusi par spilgtu piemēru uz cilvēktiesībām balstītai pieejai datu aizsardzībai.

ES datu aizsardzības regulējums sāka attīstīties, lai harmonizētu dalībvalstu datu aizsardzības režīmus un tādējādi nodrošinātu vienotu personas datu aizsardzības līmeni un brīvu datu plūsmu starp ES dalībvalstīm. Atšķirīgs tiesiskais regulējums datu aizsardzības jomā rada draudus ekonomiskajai darbībai un brīvai konkurencei ES iekšējā tirgū, kas balstās uz brīvu datu plūsmu starp dalībvalstīm. Lai novērstu šķēršļus brīvai personas datu plūsmai ES un nepieļautu, ka valstis to nepamatoti ierobežo, atsaucoties uz nepieciešamību aizsargāt personu tiesības un brīvības, īpaši tiesības uz privātumu, bija svarīgi nodrošināt vienādu pamattiesību aizsardzības līmeni visās dalībvalstīs.

1992. gada Līgumā par Eiropas Savienību pamattiesību ievērošanas princips tika atzīts par ES vispārējo tiesību principu, kā arī noteikts, ka ES respektē pamattiesības atbilstoši ECTK un dalībvalstu kopīgām konstitucionālām tradīcijām (6. pants).[368]

1995. gada 24. oktobrī Eiropas Parlaments un Padome pieņēma Direktīvu 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu

366 Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1, pp. 501–507. https://doi.org/10.1038/s42256-019-0114-4

367 Jobin, A., Ienca, M., Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, pp. 389–399. https://doi.org/10.1038/s42256-019-0088-2

368 Līgums par Eiropas Savienību, 1992. *OV C* 325, 24.12.2002.

datu brīvu apriti (Direktīva 95/46/EK).[369] Tā bija galvenais ES tiesību akts datu aizsardzības jomā līdz 2018. gadam, kad sāka piemērot VDAR. Direktīva 95/46/EK ieviesa detalizētus personas datu aizsardzības noteikumus un uzraudzības mehānismu. Tajā tika noteikti personas datu apstrādes principi, datu subjektu tiesības, pienākums garantēt datu apstrādes konfidencialitāti un drošību, kā arī noteikumi personas datu pārsūtīšanai uz trešajām valstīm. Direktīva 95/46/EK paredzēja pienākumu dalībvalstīm nodrošināt tiesiskās aizsardzības līdzekļus, sankcijas un atbildību personas datu aizsardzības pārkāpumu gadījumā. Tā uzlika pienākumu katrai dalībvalstij izveidot neatkarīgu datu aizsardzības iestādi. Tā arī ieviesa uzraudzības mehānismu – paziņošanas pienākumu, kā arī personas datu apstrādes reģistrēšanu, kuru VDAR vairs neparedz. Tika izveidota padomdevēja iestāde – Darba grupa personu aizsardzībai attiecībā uz personas datu apstrādi – jeb tā sauktā 29. panta darba grupa, kas pieņēma vadlīnijas par dažādiem personas datu aizsardzības jautājumiem. Daudzas no šīm vadlīnijām apstiprināja Eiropas Datu aizsardzības kolēģija, kas tika izveidota 29. panta darba grupas vietā līdz ar VDAR spēkā stāšanos.

Latvijā datu aizsardzības tiesības sākotnēji attīstījās, pārņemot ES tiesisko regulējumu. Lai ieviestu Direktīvu 95/46/EK, 2000. gada 6. aprīlī tika pieņemts Fizisko personu datu aizsardzības likums. Pamatojoties uz minēto likumu, tika izveidota Datu valsts inspekcija. Likums bija spēkā līdz pat 2018. gadam, kad tika uzsākta VDAR piemērošana.

Dalībvalstīm lielākoties paredzēta rīcības brīvība attiecībā uz veidu, kādā direktīvas normas pārņemt nacionālajā tiesību sistēmā. Tādējādi Direktīva 95/46/EK nenodrošināja pietiekamu datu aizsardzības regulējuma harmonizāciju. ES dalībvalstu datu aizsardzības likumi, kas tika pieņemti, lai ieviestu Direktīvu 95/46/EK, paredzēja būtiski atšķirīgus noteikumus, kā arī datu aizsardzības prakse dažādās dalībvalstīs bija atšķirīga, piemēram, attiecībā uz sodu piemērošanu, kā arī kārtību, kādā uzņēmējiem jāinformē dalībvalstis par veikto datu apstrādi.

Būtisks solis pamattiesību, to skaitā tiesību uz datu aizsardzību, attīstībā bija Hartas pieņemšana 2000. gadā, kas iezīmē pāreju no ekonomiskās uz cilvēktiesību pieeju datu aizsardzībai.

4.2.2. Tiesības uz datu aizsardzību kā atsevišķas pamattiesības

Hartā ir izmantota atšķirīga pieeja no ECTK un citiem agrāk pieņemtiem starptautiskiem cilvēktiesību dokumentiem, nosakot tiesības uz personas datu aizsardzību kā atsevišķas patstāvīgas cilvēka pamattiesības, kas ir nošķiramas no

369 Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti. *OV L* 281, 23.11.1995.

tiesībām uz privāto dzīvi. Tiesības uz privātās dzīves neaizskaramību ir noteiktas Hartas 7. pantā, bet tiesības uz personas datu aizsardzību – 8. pantā.

Hartas 8. panta 1. punktā ir vispārīgi atrunātas ikvienas personas tiesības uz savu personas datu aizsardzību, savukārt otrā daļa paredz piecas un trešā daļa vēl vienu prasību, kas ir atrodamas pirms tam pieņemtajā Direktīvā 95/46/EK, kā arī dalībvalstu datu aizsardzības tiesību aktos. Hartas 8. panta 2. punkts paredz, ka personas dati ir "jāapstrādā godprātīgi, noteiktiem mērķiem un ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos. Ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos." Savukārt 8. panta 3. punkts nosaka, ka atbilstību iepriekš minētajiem datu aizsardzības noteikumiem kontrolē neatkarīga iestāde.

ES datu aizsardzības regulējuma attīstībā izšķiroša nozīme bija Lisabonas līgumam, kas stājās spēkā 2009. gada 1. decembrī. Līdz ar Lisabonas līgumu Harta ieguva juridiski saistošu spēku. Tiesību uz datu aizsardzību kā atsevišķu pamattiesību noteikšana Hartā, kas ir primārais ES tiesību akts, liecina par ES pāreju no ekonomiskās pieejas datu aizsardzībā uz pamattiesībās balstītu pieeju.[370]

Tiesību uz datu aizsardzību kā atsevišķu pamattiesību atzīšana ES lielā mērā atbilst starptautisko cilvēktiesību zinātnieku atzītiem kritērijiem, lai tiktu ieviestas jaunas cilvēktiesības:

1) datu aizsardzība atspoguļo sociālas pamatvērtības straujajā jauno tehnoloģiju attīstības laikmetā;
2) tām zināmu laiku bijusi svarīga nozīme nacionālās, starptautiskās un starpvalstu sistēmās;
3) tās ir atbilstošas spēkā esošajam tiesību aktu kopumam nozarē;
4) ar tām tiek panākta augsta līmeņa vienošanās, vismaz ES;
5) tās rada jaunas tiesības un pienākumus.[371]

Akadēmiskajā literatūrā tiek norādīti vairāki iespējamie iemesli, kāpēc tiesības uz datu aizsardzību tika atzītas par atsevišķām pamattiesībām. Tiek norādīts, ka ES ir attīstījusies vairāk kā ekonomiska savienība, kur datu aizsardzība kā pamattiesības ir piemērojamas ne tikai attiecībā uz datu apstrādi, kas notiek komerciālos nolūkos kopējā tirgus ietvaros, lai aizsargātu iekšējo tirgu, bet tās ir kļuvušas par tiesisku prasību visā ES, tai skaitā arī attiecībā uz apstrādi tiesībaizsardzības nolūkos. Tāpat tiek atgādināts, ka tiesības uz datu aizsardzību aizsargā vērtības, kas "iziet ārpus" privātuma. Turklāt šādā veidā tiek atzītas konstitucionālās tradīcijas, kas pastāv dažās ES valstīs, piemēram, Francijā un Vācijā, kur tiesības uz datu aizsardzību netiek skatītas saistībā ar privātumu. Visbeidzot, kā pamatojums tiek minēts, ka saskaņā ar pragmatisko pieeju tiesības uz datu

370 Sk. Tzanou (2019), *The Fundamental Right to Data Protection*, p. 18.

371 Ibid., p. 20.

aizsardzību ļauj indivīdiem apzināties un izmantot savas tiesības, saskaroties ar jaunajiem izaicinājumiem, ko rada straujā tehnoloģiju attīstība.[372]

Tiesības uz datu aizsardzību un tiesības uz privātumu ir savā starpā cieši saistītas, tomēr patstāvīgas pamattiesības.[373] Rodas jautājums, kā minētās tiesības ir nodalāmas un atšķiras viena no otras.

Datu aizsardzība tiek uzskatīta par jaunākām, modernām un aktīvām tiesībām. Jebkurai personiskās informācijas jeb datu apstrādei jāatbilst datu aizsardzības pamatprasībām, piemēram, ir jāievēro noteiktas personu tiesības.[374] Tiesības uz personas datu aizsardzību stājas spēkā, kad tiek apstrādāti personas dati neatkarīgi no tā, kā tas ietekmē privātumu. Tādējādi tās ir plašākas par tiesībām uz privāto dzīvi. Ne visa datu apstrāde var radīt privātuma aizskārumu.[375]

Līdzīgi kā tiesības uz privātumu, arī tiesības uz datu aizsardzību ir saistītas un palīdz aizsargāt daudzas pamattiesības. Tiesībām uz datu aizsardzību ir būtiska nozīme tiesību uz privātumu nodrošināšanā, turklāt tās aizsargā citas vērtības, piemēram, diskriminācijas aizlieguma principa ievērošanu, paredzot ierobežojumus personu profilēšanai. Vācijā tiesības uz datu aizsardzību izriet no tiesībām uz "informācijas autonomiju". To pamatā savukārt ir tiesības uz "informācijas pašnoteikšanu", kas dod tiesības personai kontrolēt, kāda informācija par viņu tiek atklāta un kā dati tiek izmantoti.[376] Minētās tiesības izriet no cilvēka cieņas principa. Kā atklāts iepriekš, jautājums, cik lielā mērā personām ir tiesības neatklāt informāciju par sevi, ņemot vērā cilvēka cieņas prasību, kļūst arvien aktuālāks līdz ar arvien pieaugošo tendenci izmantot datu apstrādes algoritmus, lai novērotu personas identificējošu informāciju un to izmantotu, lai labāk saprastu, analizētu un paredzētu personu uzvedību.

Tajā pašā laikā tiesības uz datu aizsardzību ir šaurākas nekā tiesības uz privātumu. Privātuma jēdziens ir plašāks, jo tas ietver dažādus privātās sfēras aspektus, piemēram, reputāciju, identitāti, attiecības ar citiem un ārpasauli, fizisko un psiholoģisko integritāti, ģimenes dzīvi, mājas, elektronisko komunikāciju utt.[377] Līdz ar to tiesības uz privātumu un datu aizsardzību ir atšķirīgas tiesības. Turklāt tiek arī norādīts, ka atšķirībā no privātuma, kam ir subjektīvs raksturs, tiesības

372 Sk. Tzanou (2019), *The Fundamental Right to Data Protection*, p. 21.

373 ES Pamattiesību aģentūra, ECT, EP, EDAU (2018), Rokasgrāmata, 18. lpp.

374 Turpat, 19. lpp.

375 Turpat, 18. lpp.

376 Tzanou (2019), *The Fundamental Right to Data Protection*, p. 29.

377 Van Dijk et al. (2018), *Theory and Practice of the European Convention on Human Rights*, p. 669.

uz datu aizsardzību var uzskatīt par "objektīvāka" rakstura tiesībām, ņemot vērā to procesuālo raksturu.[378]

4.2.3. Datu aizsardzības reforma un Vispārīgā datu aizsardzības regula

Ar Lisabonas līgumu tiesības uz datu aizsardzību tika ietvertas Līgumā par Eiropas Savienības darbību (LESD), kā arī tika paplašināta ES kompetence pieņemt tiesību aktus datu aizsardzības jomā. LESD 16. panta 1. punkts paredz ikvienas personas tiesības uz savu personas datu aizsardzību. Tālāk 16. panta 2. punkts nosaka, ka Eiropas Parlaments un Padome paredz noteikumus par fizisko personu aizsardzību attiecībā uz ES iestāžu un struktūru veikto personas datu apstrādi, kā arī personas datu apstrādi, ko veic dalībvalstis saistībā ar ES tiesību aktu darbību, un noteikumus par šādu datu brīvu apriti, un ka šo noteikumu izpildi kontrolē neatkarīgas iestādes.

LESD 16. panta 2. punkts ieviesa jaunu juridisko pamatu ES tiesību aktu pieņemšanai datu aizsardzības jomā. Turklāt ar Lisabonas līgumu brīvības, drošības un tiesiskuma joma tika pielīdzināta pārējām ES jomām, kurās ES ir pilnvaras pieņemt tiesību aktus, kas bija pamatā datu aizsardzības direktīvas izstrādei policijas un tiesu iestāžu sadarbībai krimināltiesību jomā.

Datu aizsardzības tiesiskā regulējuma reforma tika veikta, lai harmonizētu, kā arī modernizētu ES pastāvošo tiesisko regulējumu, ņemot vērā būtiskās izmaiņas, ko bija radījusi informācijas un komunikācijas tehnoloģiju attīstība, jauno tehnoloģiju straujā izplatība un globalizācija kopš Direktīvas 95/46/EK pieņemšanas 1995. gadā. Tāpat bija nepieciešami jauni datu aizsardzības noteikumi, lai cīnītos ar terorisma un noziedzības radītajām problēmām.

Datu aizsardzības reformu Eiropas Komisija ierosināja 2012. gadā, kad tā nāca klajā ar priekšlikumu tiesību aktu paketei, kurā ietilpa VDAR un Policijas direktīva. Pēc ilga likumdošanas procesa abi ES tiesību akti tika pieņemti 2016. gadā un ir piemērojami no 2018. gada maija. Jaunā datu aizsardzības tiesiskā regulējuma pieņemšana ir nozīmīgs solis, lai sasniegtu 2015. gada Digitālā vienotā tirgus stratēģijas[379] mērķus – palielinātu uzticību digitālajiem pakalpojumiem un to drošību.

VDAR, kas piemērojama no 2018. gada 25. maija, aizstāj Direktīvu 95/46/EK un paredz vienotus noteikumus, kuri tieši piemērojami visās ES dalībvalstīs. Tās

378 Tzanou, M. (2013). Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 3(2), https://doi.org/10.1093/idpl/ipt004

379 Eiropas Komisija. (2015). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Digitālā vienotā tirgus stratēģija Eiropai. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex%3A52015DC0192

uzdevums ir stiprināt pamattiesības digitālajā laikmetā, ļaujot fiziskām personām kontrolēt savus personas datus, un vienlaikus nodrošināt brīvu datu plūsmu un ļaut uzņēmējiem maksimāli izmantot digitālā vienotā tirgus sniegtās priekšrocības, mazinot birokrātiju un veicinot patērētāju uzticību.

VDAR ir nostiprināti Direktīvā 95/46/EK noteiktie personas datu aizsardzības principi un datu subjektu tiesības, tās attīstot un papildinot. VDAR piešķir arī ES un dalībvalstīm iespēju tiesību aktos noteikt ierobežojumus datu subjekta tiesību un pienākumu darbībai, to starpā attiecībā uz pārziņa pienākumu ziņot datu subjektam par personas datu aizsardzības pārkāpumiem un personas datu apstrādes principu piemērošanu, ja šādi ierobežojumi ir nepieciešami demokrātiskā sabiedrībā un samērīgi, lai garantētu būtiskus sabiedrības interešu mērķus, piemēram, valsts drošību, aizsardzību, sabiedrisko drošību, vai lai aizstāvētu citu personu tiesības un brīvības (23. panta 1. punkts). Paredzot šādus ierobežojumus, tiesību aktā ir jāietver arī konkrēti noteikumi par datu apstrādi, lai garantētu likumīgu un godprātīgu apstrādi (VDAR 23. panta 2. punkts).

VDAR nosaka vispārīgu pienākumu uzņēmumiem un organizācijām veikt "atbilstošus tehniskus un organizatoriskus pasākumus", lai aizsargātu personas datus, kā arī nosaka konkrētus pasākumus, kas jāveic, lai nodrošinātu atbilstību VDAR, to skaitā reģistrēt apstrādes darbības (30. pants), veikt novērtējumu par šo darbību ietekmi uz datu aizsardzību (35. pants), ieviest atbilstošus drošības pasākumus (32. pants), iecelt datu aizsardzības speciālistu (37. pants), ziņot par datu aizsardzības pārkāpumiem (33. un 34. pants).

Pārzinim[380] ir arī jāīsteno atbilstīga personas datu pārvaldības politika, ciktāl tas ir samērīgi ar apstrādes darbībām. VDAR ir noteikta uz risku balstīta pieeja, kas paredz, ka pasākumi ir jāīsteno, ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūku, kā arī paredz dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām. Tādējādi tie var atšķirties katrā konkrētajā gadījumā, un pašam pārzinim ir jānosaka, kādi pasākumi ir nepieciešami. Šādi pasākumi var būt iekšējo procedūru, piemēram, personas datu aizsardzības politikas, pieņemšana un ieviešana praksē, atbildīgo personu nozīmēšana, regulāras apmācības utt.

Pārzinim ir pienākums kontrolēt personas datus, arī uzticot tos citiem, piemēram, glabāšanai. VDAR nosaka pienākumu pārzinim izmantot tikai tādus apstrādātājus[381], kas sniedz pietiekamas garantijas, ka tiks īstenoti atbilstoši tehniskie

380 VDAR 4. panta 7. punkts nosaka, ka pārzinis ir "fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus".

381 VDAR 4. panta 8. punkts nosaka, ka apstrādātājs ir "fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus".

un organizatoriskie pasākumi tādā veidā, lai apstrādē tiktu ievērotas VDAR prasības un tiktu nodrošināta datu subjekta tiesību aizsardzība (28. panta 1. punkts).

VDAR paredz vairākus būtiskus jaunievedumus. Tā ievieš integrētas datu aizsardzības principu un datu aizsardzības pēc noklusējuma principu, pārredzamības principu un tiesības uz datu pārnesamību. VDAR uzliek pienākumu noteiktos gadījumos veikt novērtējumu par ietekmi uz datu aizsardzību, kā arī nozīmēt datu aizsardzības speciālistu. Vienlaikus tā atceļ iepriekš pastāvošo personas datu apstrādes reģistrēšanu uzraudzības iestādēs. Detalizētāk datu aizsardzības prasības un to piemērošana attiecībā uz mākslīgā intelekta novērošanas pasākumiem apskatīta grāmatas sestajā nodaļā.

VDAR ir tieši piemērojama visās dalībvalstīs, un tā nav jāievieš nacionālajā regulējumā, tādējādi tiek izveidoti vienoti personas datu aizsardzības noteikumi, kas ir spēkā visā ES. Tajā pašā laikā VDAR ir paredzēti noteikumi, kurus var konkretizēt vai ierobežot ar dalībvalstu tiesību aktiem.[382] Tā satur vairāk nekā piecdesmit tā sauktās "atvērtās normas", kuras vai nu uzliek pienākumu dalībvalstīm pieņemt īpašus noteikumus[383], vai arī paredz dalībvalstīm rīcības brīvību un atļauj papildināt, konkretizēt vai paredzēt izņēmumus no VDAR[384]. Dalībvalstu tiesiskais regulējums nedrīkst traucēt VDAR noteikumu vienveidīgu piemērošanu visā ES.[385]

Latvija Fizisko personu datu apstrādes likumu (FPDAL) pieņēma 2018. gada 21. jūnijā.[386] FPDAL 8. nodaļā ir paredzēti specifiskie noteikumi un izņēmumi no datu subjektu tiesībām. Datu subjektam nav tiesību saņemt informāciju, ja to ir aizliegts izpaust saskaņā ar normatīvajiem aktiem, piemēram, nacionālās drošības, valsts aizsardzības, sabiedrības drošības un krimināltiesību jomā utt. (27. panta pirmā daļa). Ierobežots ir arī piekļuves tiesību īstenošanas termiņš – datu

382 VDAR 8. apsvērums.

383 Piemēram, noteikumi par rīcības kodeksiem – VDAR 40. pants, sertifikāciju – 42. pants, uzraudzības iestādes izveidi un pilnvarām – 54. pants un 58. panta 1. punkts.

384 Piemēram, normas, kas attiecas uz apstrādes tiesisko pamatu – VDAR 6. panta 2. un 3. punkts, bērna piekrišanu attiecībā uz informācijas sabiedrības pakalpojumiem – 8. panta 1. punkts, īpašo kategoriju personas datu apstrādi – 9. panta 2., 3., 4. punkts, personas datu par sodāmību un pārkāpumiem apstrāde – 10. pants, datu subjektu tiesību ierobežojumiem konkrētos gadījumos – 23. pants, apstrādi saistībā ar nodarbinātību – 88. pants.

385 VDAR 10. apsvērums. EST 1978. gada 31. janvāra spriedums lieta 94/77 *Fratelli Zerbone Snc pret Amministrazione delle finanze dello Stato*, ECLI:EU:C:1978:17, 25. punkts.

386 Fizisko personu datu apstrādes likums. Pieņemts 21.06.2018. *Latvijas Vēstnesis*, 04.07.2018., Nr. 132. Tas nosaka vispārīgos noteikumus (1. nodaļa), Datu valsts inspekcijas uzdevumus un statusu (2. nodaļa), inspekcijas darbības organizāciju (3. nodaļa), pārbaužu īstenošanas kārtību (4. nodaļa), noteikumus attiecībā uz datu aizsardzības speciālistiem (5. nodaļa), sertifikācijas un rīcības kodeksu pārraudzības institūcijas (6. nodaļa), lēmumu pieņemšanas, apstrīdēšanas un pārsūdzēšanas kārtību (7. nodaļa), datu apstrādi un datu subjekta tiesības (8. nodaļa).

subjekts var saņemt informāciju par tā datu saņēmējiem vai saņēmēju kategorijām, kam dati ir izpausti pēdējo divu gadu laikā (27. panta otrā daļa). FPDAL paredz speciālus noteikumus un datu subjektu tiesību ierobežojumus attiecībā uz īpašām apstrādes situācijām, piemēram, datu apstrādi saistībā ar vārda un informācijas brīvību (32. pants), kā arī datu apstrādi krimināltiesību jomā, nosakot, ka datu apstrāde sākotnēji neparedzētiem mērķiem krimināltiesību jomā ir pieļaujama, lai novērstu tūlītēju būtisku sabiedriskās drošības apdraudējumu, vai saskaņā ar speciālo regulējumu (34. pants). Speciālie noteikumi un izņēmumi var tikt paredzēti citos normatīvajos aktos, nodrošinot atbilstošas garantijas datu subjekta tiesībām un brīvībām un ievērojot VDAR noteiktās prasības.

4.2.4. Speciālais datu aizsardzības regulējums

Līdzās VDAR, kas paredz vispārīgo datu aizsardzības regulējumu, ES ir pieņēmusi vairākus speciālos tiesību aktus jeb *lex specialis*, kas konkretizē un papildina VDAR noteikumus.

Vienlaikus ar VDAR tika pieņemta Policijas direktīva, kuru dalībvalstīm ir pienākums ieviest nacionālajā regulējumā. Tā paredz speciālus noteikumus par personas datu apstrādi krimināllizmeklēšanas un tiesībaizsardzības nolūkos. Policijas direktīvas uzdevums ir stiprināt personu tiesību aizsardzību attiecībās ar tiesībaizsardzības iestādēm, kā arī efektīvāk apkarot noziedzību un terorismu visā ES, atvieglojot tiesībaizsardzības iestāžu pārrobežu sadarbību.

Lai pārņemtu Policijas direktīvas prasības, Latvija 2019. gada 8. jūlijā pieņēma likumu "Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā"[387]. Likuma mērķis ir aizsargāt fizisko personu pamattiesības un brīvības, it īpaši privātās dzīves neaizskaramību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus un administratīvos pārkāpumus, lai izpildītu krimināl sodus un administratīvos sodus, kā arī lai veiktu citas ar administratīvā pārkāpuma procesu un krimināl procesu saistītās darbības (2. pants). Likumu piemēro tikai attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes iepriekš minētajos nolūkos, savukārt, ja tiesību aizsardzības iestādes veic apstrādi citos nolūkos, uz to ir attiecināmas VDAR normas.

Speciālos datu aizsardzības noteikumus paredz arī Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi

387 Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā. LV likums. Pieņemts 08.07.2019. *Latvijas Vēstnesis*, 22.07.2019., Nr. 147.

un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (E-privātuma direktīva).[388]

E-privātuma direktīva aizsargā Hartas 7. pantā nostiprinātās tiesības uz privāto dzīvi, kuru būtiska sastāvdaļa ir elektronisko sakaru konfidencialitāte. Tās uzdevums ir garantēt elektronisko sakaru datu, aprīkojuma un pakalpojumu brīvu apriti ES. E-privātuma direktīva uzliek pienākumu publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem nodrošināt tīkla drošību, komunikāciju un informācijas par datu plūsmu konfidencialitāti. Tajā pašā laikā E-privātuma direktīva ir attiecināma tikai uz tradicionālajiem elektronisko sakaru pakalpojumiem, bet neattiecas uz jaunajiem elektronisko sakaru pakalpojumu sniedzējiem, piemēram, "WhatsApp", "Facebook Messenger", "Skype", "Gmail" u. c., kurus līdz ar tehnoloģiju progresu arvien vairāk izmanto kā patērētāji, tā uzņēmumi.

Speciālais datu aizsardzības regulējums attiecībā uz elektronisko sakaru konfidencialitātes aizsardzību, pārņemot E-privātuma direktīvas prasības, Latvijā tika ietverts Elektronisko sakaru likumā[389] un Informācijas sabiedrības pakalpojumu likumā[390]. Likums paredz elektronisko sakaru komersanta pienākumu nodrošināt saglabājamo datu glabāšanu 18 mēnešus un nodot tos tiesībaizsardzības iestādēm – pirmstiesas izmeklēšanas iestādēm, operatīvās darbības subjektiem, valsts drošības iestādēm, prokuratūrai un tiesai –, lai aizsargātu valsts un sabiedrisko drošību vai nodrošinātu noziedzīgu nodarījumu izmeklēšanu, kriminālvajāšanu un krimināllietu iztiesāšanu, kā arī Konkurences padomei, izmeklējot konkurences tiesību pārkāpumus, kas izpaužas kā aizliegtas vienošanās (19. panta pirmās daļas 11. punkts, 71.[1] pants).

Kā paredzēts 2015. gada Digitālajā vienotā tirgus stratēģijā Eiropai, 2016. gadā tika paziņots par E-privātuma direktīvas pārskatīšanu, lai nodrošinātu augsta līmeņa privātuma aizsardzību elektronisko sakaru pakalpojumu lietotājiem un vienlīdzīgus konkurences apstākļus visiem tirgus dalībniekiem, kā arī atbilstību VDAR.[391] 2017. gada 10. janvārī Eiropas Komisija pieņēma priekšlikumu Regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā, ar ko atceļ Direktīvu 2002/58/EK (E-privātuma regulas

388 Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektronisko komunikāciju). *OV L* 201, 31.07.2002.

389 Elektronisko sakaru likums. Pieņemts 28.10.2004. *Latvijas Vēstnesis*, 17.11.2004., Nr. 183.

390 Informācijas sabiedrības pakalpojumu likums. Pieņemts 04.11.2004. *Latvijas Vēstnesis*, 17.11.2004., Nr. 183.

391 Eiropas Komisija (2015), Komisijas paziņojums .. Digitālā vienotā tirgus stratēģija Eiropai.

priekšlikums).[392] E-privātuma regula konkretizēs un papildinās VDAR noteikumus attiecībā uz elektronisko sakaru datiem, kuri kvalificējami kā personas dati. Ar to paredzēts nodrošināt augstu aizsardzības līmeni gan saturam, gan metadatiem un paplašināt konfidencialitātes pienākumu, aptverot ne tikai tradicionālos sakaru pakalpojumus, bet arī citus esošos un nākotnes saziņas līdzekļus, tostarp piekļuvi internetam, tūlītējās ziņapmaiņas lietojumprogrammas, e-pastu, interneta tālruņa zvanus un personīgo ziņapmaiņu sociālajos medijos. Tā paredz regulēt sīkdatnes un piekrišanas noteikumus to izmantošanai. E-privātuma regulas pieņemšanas process ir ilgs, mēģinot panākt kompromisus un nodrošināt atbilstību VDAR. 2019. gadā EDRi kopā ar četrām citām pilsoniskās sabiedrības organizācijām uzsvēra steidzamu nepieciešamību pēc stingras E-privātuma regulas, lai risinātu problēmas, ko rada komerciālās novērošanas uzņēmējdarbības modeļi, un vērsa uzmanību, ka šie modeļi, kas balstīti uz cilvēku personīgās dzīves mirkļu izsekošanu, ir pārņēmuši internetu un radījuši stimulus, lai veicinātu dezinformāciju, manipulācijas un nelegālu saturu.[393] Gan Eiropas Datu aizsardzības uzraudzītājs, gan Eiropas Datu aizsardzības kolēģija atgādina, ka jaunajai regulai būtu jāsniedz vienāds vai augstāks aizsardzības līmenis nekā VDAR, nevis zemāks.[394]

Vēl ir arī daudzi citi speciālie tiesību akti, kas ietver datu aizsardzības noteikumus. 2018. gada oktobrī tika pieņemts jauns regulējums, kas ir piemērojams attiecībā uz personas datu apstrādi ES iestādēs un struktūrās – Regula Nr. 2018/1725[395]. Šādu apstrādi kontrolē Eiropas Datu aizsardzības uzraudzītājs. Datu aizsardzības noteikumus attiecībā uz konkrētām datu apstrādes darbībām tiesībaizsardzības jomā ietver arī Regula 2016/794 par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu), kas tiek uzskatīta par informācijas apmaiņas centru Eiropas

392 Eiropas Komisija. (2017). Priekšlikums. Eiropas Parlamenta un Padomes regula par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula). https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX:52017PC0010

393 Open letter to EU Member States. (11 October, 2019). *EDRi.* https://edri.org/files/eprivacy/ePrivacy_NGO_letter_20191011.pdf

394 Buttarelli, G. (19 October, 2018). The urgent case for a new ePrivacy law. *EDPS*. https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en; EDPB. (2019). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

395 Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK. *OV L* 295/39, 21.11.2018.

Savienībā.[396] Informācija, ko Eiropols vāc, glabā, apstrādā, analizē un ar ko tas apmainās, aptver kriminālizlūkošanu saistībā ar informāciju par noziegumiem vai noziedzīgām darbībām, kuru apkarošana ietilpst Eiropola mērķu darbības jomā, un informāciju, kura iegūta, lai noteiktu, vai ir izdarīti konkrēti noziedzīgi nodarījumi vai arī tie varētu tikt izdarīti nākotnē (12. apsvērums). Datu aizsardzības noteikumus ietver arī Padomes Regula (ES) 2017/1939, ar ko īsteno ciešāku sadarbību Eiropas Prokuratūras (EPPO) izveidei,[397] Regula (ES) 2018/1727 par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (Eurojust).[398]

Datu aizsardzības regulējumu ietekmē arī ES pieņemtais regulējums citās jomās, to skaitā kiberdrošībā. Drīz pēc VDAR pieņemšanas, 2016. gada jūlijā, tika pieņemta Direktīva 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (tā sauktā NIS direktīva)[399]. Lai pārņemtu minēto direktīvu, Latvija 2018. gadā veica būtiskus grozījumus 2010. gadā pieņemtajā Informācijas tehnoloģiju drošības likumā[400] un pieņēma 2015. gada Ministru kabineta noteikumus Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām".[401] 2019. gadā tika pieņemts Kiberdrošības akts, kas paredz ieviest ES mēroga kiberdrošības sertifikāciju, lai nodrošinātu, ka informāciju un komunikāciju tehnoloģiju produkti, pakalpojumi un procesi atbilst drošības standartiem, kā arī paredz stiprināt Eiropas Savienības Kiberdrošības aģentūras (ENISA) pilnvaras.[402]

396 Eiropas Parlamenta un Padomes Regula (ES) 2016/794 (2016. gada 11. maijs) par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu) un ar kuru aizstāj un atceļ Padomes Lēmumus 2009/371/TI, 2009/934/TI, 2009/935/TI, 2009/936/TI un 2009/968/TI. *OV L* 135, 24.05.2016.

397 Padomes Regula (ES) 2017/1939 (2017. gada 12. oktobris), ar ko īsteno ciešāku sadarbību Eiropas Prokuratūras (EPPO) izveidei. *OV L* 283, 31.10.2017.

398 Eiropas Parlamenta un Padomes Regula (ES) 2018/1727 (2018. gada 14. novembris) par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (Eurojust) un ar ko aizstāj un atceļ Padomes Lēmumu 2002/187/TI. *OV L* 295, 21.11.2018.

399 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā. *OJ L* 194, 19.07.2016.

400 Informācijas tehnoloģiju drošības likums. Pieņemts 28.10.2010. *Latvijas Vēstnesis*, 10.11.2010., Nr. 178.

401 MK noteikumi Nr. 442. Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām. Pieņemti 2015. gada 28. jūlijā. *Latvijas Vēstnesis*, 03.08.2015., Nr. 149.

402 Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (Dokuments attiecas uz EEZ). *OV L* 151, 07.06.2019.

Līdzās personas datu aizsardzības regulējumam Digitālā vienotā tirgus stratēģijas ietvaros ES ir pieņēmusi vairākus tiesību aktus, lai veicinātu uz datiem orientētas ekonomikas attīstību. 2018. gadā tika pieņemta Regula par nepersonalizētu datu brīvu apriti[403] un 2019. gadā – Direktīva par atvērtajiem datiem[404].

2020. gada februārī Eiropas Komisija pieņēma divus paziņojumus: Eiropas digitālās nākotnes veidošana[405], kā arī Eiropas datu stratēģiju[406], kas iepazīstina ar redzējumu par vienotu Eiropas datu telpu. Minētajos dokumentos tiek uzsvērts, ka tehnoloģiju, to skaitā mākslīgā intelekta, attīstībai, kā arī starptautiskajai sadarbībai šajā jomā ir jābalstās uz vērtībām un pamattiesībām, ieskaitot cilvēka cieņu, nediskrimināciju, privātās dzīves un datu aizsardzību.

2022. gada 30. maijā tika pieņemta Eiropas Parlamenta un Padomes Regula (ES) 2022/868 par Eiropas datu pārvaldību jeb Datu pārvaldības akts[407], kas paredz uzlabot nosacījumus datu kopīgošanai iekšējā tirgū, palielināt datu pieejamību un novērst tehniskos šķēršļus datu atkārtotai izmantošanai.

2022. gada februārī Eiropas Komisija publicēja Priekšlikumu Eiropas Parlamenta un Padomes regulai par saskaņotiem noteikumiem par taisnīgu piekļuvi datiem un to lietošanu (Datu aktu)[408], kura mērķis ir veicināt uzņēmumu un patērētāju labāku piekļuvi datiem un to izmantošanu, sniegt iespēju valsts iestādēm piekļūt privātā sektora datiem, ļaut klientiem pārslēgties starp dažādiem mākoņpakalpojumu sniedzējiem.

2020. gada 15. decembrī Eiropas Komisija nāca klajā ar Digitālo pakalpojumu akta pakotni, kas sastāvēja no divu regulu projektiem. Abas regulas tika

403 Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā. *OV L* 303/59, 28.11.2018. Regulas mērķis ir likvidēt šķēršļus brīvai datu pārrobežu plūsmai, jo īpaši dalībvalstu bieži piemērotos datu atrašanās vietas ierobežojumus. Tā kopā ar jau spēkā esošo personas datu aizsardzības regulējumu vairos juridisko noteiktību datu uzglabāšanas un citādas apstrādes pakalpojumu un darbību tirgū, ļaujot izmantot jauno tehnoloģiju radītās priekšrocības.

404 Eiropas Parlamenta un Padomes Direktīva (ES) 2019/1024 (2019. gada 20. jūnijs) par atvērtajiem datiem un publiskā sektora informācijas atkalizmantošanu. *OV L* 172, 26.06.2019.

405 Eiropas Komisija (2020). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Eiropas digitālās nākotnes veidošana. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52020DC0067

406 Eiropas Komisija (2020). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Eiropas Datu stratēģija. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52020DC0066

407 Eiropas Parlamenta un Padomes Regula (ES) 2022/868 (2022. gada 30. maijs) par Eiropas datu pārvaldību un ar ko groza Regulu (ES) 2018/1724 (Datu pārvaldības akts) (Dokuments attiecas uz EEZ). *OV L* 152, 03.06.2022.

408 Eiropas Komisija. (2020). Priekšlikums. Eiropas Parlamenta un Padomes regula par saskaņotiem noteikumiem par taisnīgu piekļuvi datiem un to lietošanu (Datu akts). https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52022PC0068

pieņemtas 2022. gada 5. jūlijā. Tās ir: Eiropas Parlamenta un Padomes Regula (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts)[409], ko piemēros no 2024. gada 17. februāra, un Eiropas Parlamenta un Padomes Regula (ES) 2022/1925 (2022. gada 14. septembris) par sāncensīgiem un godīgiem tirgiem digitālajā nozarē un ar ko groza Direktīvas (ES) 2019/1937 un (ES) 2020/1828 (Digitālo tirgu akts) [410], ko piemēro no 2023. gada 2. maija. Jaunais regulējums būs tieši piemērojams visās ES dalībvalstīs un radīs drošāku un atvērtāku digitālo vidi, kas balstās pamattiesībās. Tas ļaus cilvēkiem kontrolēt to, ko viņi redz internetā, lai tie nebūtu ierobežoti ar saturu, ko tiem izvēlas rādīt lielo tehnoloģiju platformu izstrādātie algoritmi.

Digitālo pakalpojumu akts nosaka skaidrus pienākumus digitālo pakalpojumu sniedzējiem, piemēram, sociālajiem medijiem un uzņēmumiem, kuri nodarbojas ar tiešsaistes tirdzniecību, lai novērstu nelikumīga, kaitīga un dezinformējoša satura izplatību. Jaunās prasības ir samērīgas ar platformu lielumu un riskiem, ko tās rada. Jaunā regula paredz pasākumus, lai cīnītos pret nelikumīgu saturu tiešsaistē, un uzliek platformām pienākumu ātri uz to reaģēt, vienlaikus ievērojot pamattiesības, tostarp vārda brīvību un datu aizsardzību. Tas paredz platformu pārredzamības un atbildības prasības, piemēram, pienākumu sniegt skaidru informāciju par satura moderēšanu un algoritmu izmantošanu satura ieteikšanai (tā sauktajām ieteikumu sistēmām). Digitālo pakalpojumu akts paredz nodrošināt lietotājiem efektīvus aizsardzības pasākumus, tostarp iespēju apstrīdēt platformu satura moderēšanas lēmumus, un nosaka obligāti sniedzamu informāciju lietotājiem, kad viņu saturs tiek izņemts vai ierobežots. Tas aizliedz maldinošu praksi, kuras mērķis ir manipulēt ar lietotāju izvēli, un noteikta veida mērķorientētas reklāmas, piemēram, izmantojot nepilngadīgo personu datus, kā arī sensitīvus datus. Ļoti lielām tiešsaistes platformām un meklētājprogrammām (ar 45 miljoniem vai vairāk ikmēneša lietotāju), būs jāievēro stingrāki pienākumi, ko uzraudzīs Eiropas Komisija, to skaitā jāanalizē un jānovērš sistēmiski riski (piemēram, nelikumīga satura izplatīšana; negatīva ietekme uz pamattiesībām; negatīva ietekme uz demokrātiskiem procesiem un sabiedrisko drošību; negatīva ietekme uz sabiedrības veselības aizsardzību un nepilngadīgajiem) un jāveic neatkarīga revīzija. Šīm lielajām platformām būs jāpiedāvā lietotājiem tāda satura ieteikšanas sistēma, kas nav balstīta uz viņu profilēšanu. Tām būs arī pienākums

409 Eiropas Parlamenta un Padomes Regula (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts) (Dokuments attiecas uz EEZ). *OV L* 227, 27.10.2022.

410 Eiropas Parlamenta un Padomes Regula (ES) 2022/1925 (2022. gada 14. septembris) par sāncensīgiem un godīgiem tirgiem digitālajā nozarē un ar ko groza Direktīvas (ES) 2019/1937 un (ES) 2020/1828 (Digitālo tirgu akts) (Dokuments attiecas uz EEZ). *OV L* 265, 12.10.2022.

atvieglot iestādēm un pētniekiem piekļuvi saviem datiem un algoritmiem, lai tos varētu pārbaudītu. Šis akts paredz būtiskus mehānismus, lai nodrošinātu platformu atbildību, tomēr ir daudzi izaicinājumi, kas saistīti ar tā ieviešanu un piemērošanu praksē.

Digitālo tirgu akts savukārt paredz noteikumus lielajām tiešsaistes platformām, kas darbojas kā vārtziņi jeb piekļuves kontrolieri (*gatekeepers* – angļu val.). Tā mērķis ir panākt, lai šīs platformas darbotos taisnīgi tiešsaistē, tādējādi nodrošinot taisnīgu komercvidi komerciālajiem lietotājiem, kuri ir atkarīgi no piekļuves kontrolieriem attiecībā uz savu pakalpojumu piedāvāšanu vienotajā tirgū, tehnoloģiju jaunuzņēmējiem, kā arī patērētājiem. Piemēram, šī regula aizliedz piekļuves kontrolieriem piemērot labvēlīgākus ierindošanas noteikumus pakalpojumiem un produktiem, kurus viņi piedāvā, salīdzinājumā ar citiem līdzīgiem pakalpojumiem un produktiem, ko piedāvā trešās personas viņu platformā. Šī regula arī papildina datu aizsardzības regulējumu, piemēram, attiecībā uz patērētāju profilēšanu, paredzot aizliegumu bez gala lietotāja iepriekšējas piekrišanas izsekot tos ārpus piekļuves kontrolieru pamatplatformas pakalpojuma, lai piedāvātu mērķorientētas reklāmas.

Lai gan ES datu aizsardzības reformas rezultātā ES ir pieņemti daudzi jauni tiesību akti, tajā pašā laikā tie neveido pilnīgi vienotu sistēmu. ES institūcijas, tāpat kā dalībvalstis, nav vēl pārskatījusi visus tiesību aktus, kas pieņemti pirms VDAR un Policijas direktīvas pieņemšanas un ietver speciālos datu aizsardzības noteikumus.[411] Turklāt datu aizsardzības regulējumu ietekmē jaunais regulējums, tai skaitā iepriekš aplūkotais Digitālo tirgu akts un Digitālo pakalpojumu akts. Datu aizsardzības regulējumu būtiski ietekmē arī mākslīgā intelekta regulējuma attīstība. ES uz pamattiesībām balstītā pieeja, kas ir pamatā datu aizsardzības regulējuma attīstībai, nosaka arī mākslīgā intelekta tehnoloģiju regulējuma turpmāko attīstību.

4.2.5. Mākslīgā intelekta regulējuma attīstība

Līdzīgi kā citas starptautiskās organizācijas, arī ES ir veikusi būtiskus soļus, lai izstrādātu mākslīgā intelekta ētisko un tiesisko regulējumu. 2018. gada aprīlī Eiropas Komisija publicēja paziņojumu "Mākslīgais intelekts Eiropai"[412] – pirmo ES mākslīgā intelekta stratēģiju, kas nosaka trīs galvenās prioritātes. Pirmkārt,

411 Sk. Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement; Drechsler, L. (2021). Wanted: LED adequacy decisions How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context, *International Data Privacy Law*, 11(2), pp. 182–195. https://doi.org/10.1093/idpl/ipaa019

412 Eiropas Komisija (2018), Komisijas paziņojums. Mākslīgais intelekts Eiropai.

veicināt ES tehnoloģisko attīstību un mākslīgā intelekta izmantošanu valsts un privātajā sektorā. Otrkārt, sagatavoties sociāli ekonomiskajām pārmaiņām, ko rada mākslīgais intelekts. Treškārt, izveidot atbilstošu ētisko un tiesisko regulējumu, pamatojoties uz ES vērtībām un saskaņā ar Hartu.

Mākslīgā intelekta kā ES līmeņa politikas prioritātes attīstība ir saistīta ar diskusiju, kā veicināt uzticēšanos mākslīgā intelekta sistēmām un kā nodrošināt, lai to izstrāde vai ieviešana neapdraud ES pamattiesības. Šie jautājumi patiesībā nav pilnīgi jauni, bet balstās iepriekšējās juridiskajās un politiskajās debatēs par pamattiesībām, un tie galvenokārt saistīti ar lielajiem datiem, kā arī vispārīgāk – ar datu apstrādes regulējumu.[413]

2018. gada 7. decembrī Eiropas Komisija pieņēma Mākslīgā intelekta koordinēto plānu[414], kas aicināja ES dalībvalstis sagatavot nacionālās stratēģijas mākslīgā intelekta jomā. Līdzīgi kā citas valstis, arī Latvija izstrādāja šādu stratēģiju. 2020. gada 4. decembrī Ministru kabinets apstiprināja Vides aizsardzības un reģionālās attīstības ministrijas sagatavoto informatīvo ziņojumu "Par mākslīgā intelekta risinājumu attīstību"[415].

ES uzsāka risināt mākslīgā intelekta ētiskos un juridiskos izaicinājumus, izveidojot divas darba grupas – AI HLEG un Atbildības un jauno tehnoloģiju ekspertu grupu. 2018. gada jūnijā tika izveidota AI HLEG, un 52 augsta līmeņa ekspertiem, kas tajā darbojās, tika uzticēts izstrādāt ieteikumus par mākslīgā intelekta politikas attīstību un ētiskiem, juridiskiem un sociāliem jautājumiem, kas nodrošinātu Eiropas mākslīgā intelekta stratēģijas un koordinētā plāna īstenošanu, pamatojoties uz cilvēku vērstu un ētisku pieeju mākslīgajam intelektam.

Pēc gada, 2019. gada aprīlī, AI HLEG pieņēma Ētikas vadlīnijas uzticamam mākslīgajam intelektam (MI ētikas vadlīnijas)[416]. Tajās ir uzsvērts – lai mākslīgā intelekta sistēmas varētu uzskatīt par uzticamām, tām ir jāatbilst trīs pazīmēm, proti, tām ir jābūt

1) likumīgām – jāievēro visi piemērojamie tiesību akti un pamattiesības;
2) ētiskām – jānodrošina ētikas principu un vērtību ievērošana;
3) noturīgām no tehniskā un sociālā viedokļa.

Lai mākslīgā intelekta sistēmas atbilstu ētiskuma pazīmei, tās ir jāizstrādā, jāievieš un jāizmanto, pamatojoties uz pamattiesībās balstītu pieeju un ievērojot

413 Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement.

414 Eiropas Komisija. (2018). Komisijas paziņojums Eiropas Parlamentam, Eiropadomei, Padomei, Eiropas Ekonomikas un Sociālajai komitejai un Reģionu komitejai. Koordinētais mākslīgā intelekta plāns. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52018DC0795&from=EN

415 VARAM (2020), Informatīvais ziņojums "Par mākslīgā intelekta risinājumu attīstību".

416 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

četrus ētikas principus: cilvēka patstāvība; kaitējuma novēršana; taisnīgums un izskaidrojamība.

MI ētikas vadlīnijas nosaka arī septiņas pamatprasības, kas ir jānodrošina, lai mākslīgā intelekta sistēmu izstrāde, ieviešana un izmantošana atbilstu uzticama mākslīgā intelekta prasībām:

1) cilvēka subjektība un virsvadība (cilvēka spēja pieņemt patstāvīgus lēmumus saistībā ar mākslīgo intelektu un šo sistēmu virsvadība);
2) tehniskā noturība un drošums;
3) privātums un datu pārvaldīšana;
4) pārredzamība;
5) daudzveidība, nediskriminēšana un taisnīgums;
6) vides un sabiedrības labklājība;
7) atbildīgums.

Pamatnostādnēs sniegts arī novērtēšanas saraksts, lai palīdzētu praktiski īstenot minētās prasības.

MI ētikas vadlīnijās kā viena no mākslīgā intelekta kritiskajām problēmjomām ir norādīta fizisku personu identificēšana un izsekošana, izmantojot mākslīgā intelekta sistēmas. Tās ļauj gan publiskām, gan privātām struktūrām arvien efektīvāk identificēt konkrētas personas. Vērā ņemami mākslīgā intelekta identifikācijas piemēri ir sejas atpazīšana un citas piespiedu identifikācijas metodes, kas izmanto biometriskos datus, piemēram, melu atpazīšana, personības vērtēšana ar mikroizpausmju palīdzību, automātiska balss atpazīšana. Dažkārt fizisku personu identificēšana ir vēlama un atbilst ētikas principiem, piemēram, ja to izmanto, lai atklātu krāpšanu, nelikumīgi iegūtu līdzekļu legalizāciju vai terorisma finansēšanu. Tomēr automātiska identificēšana raisa būtiskas juridiskas un ētiskas bažas, un tai var būt neparedzēta ietekme daudzos psiholoģiskos un sociālkulturālos līmeņos. Lai nosargātu Eiropas pilsoņu patstāvību, ir nepieciešams samērīgi izmantot mākslīgā intelekta kontroles paņēmienus. Uzticama mākslīgā intelekta sasniegšanai būs ļoti svarīgi skaidri definēt, vai, kad un kā mākslīgo intelektu var izmantot, lai automātiski identificētu cilvēkus, un nošķirt personas identificēšanu no tās izsekošanas, kā arī mērķtiecīgu novērošanu no masveida novērošanas. Šādu tehnoloģiju izmantošana ir skaidri jāpamato saskaņā ar spēkā esošajiem tiesību aktiem.

MI ētikas vadlīnijās kā vēl viena problēmjoma tiek norādīta mākslīgā intelekta atbalstīta iedzīvotāju vērtēšana, kas pārkāpj pamattiesības. Jebkāda iedzīvotāju vērtēšana var novest pie patstāvības zaudējuma un apdraudēt nediskriminēšanas principu. Vērtēšana būtu jāizmanto tikai tad, ja tā ir pamatota un ja pasākumi ir samērīgi un taisnīgi. Valsts iestāžu vai privātā sektora veikta iedzīvotāju vērtēšana (vispārējs "morālās personības" vai "ētiskās godprātības" vērtējums) visos aspektos un plašā mērogā apdraud šīs vērtības, jo īpaši, ja to neizmanto saskaņā

ar pamattiesībām vai ja to izmanto nesamērīgi, bez skaidri noteikta un paziņota leģitīmā mērķa.

2019. gada aprīlī kopā ar MI ētikas vadlīniju pārskatīto versiju tika publicēts Eiropas Komisijas paziņojums "Uzticības veidošana uz cilvēku vērstam mākslīgajam intelektam"[417], kas uzsāka visaptverošu izmēģināšanas procesu, iesaistot plašu ieinteresēto personu loku, lai pārbaudītu MI vadlīniju praktisku īstenošanu mākslīgā intelekta sistēmu izstrādē un izmantošanā.

2019. gada jūnijā AI HLEG publicēja otru dokumentu – "Politikas un ieguldījumu ieteikumi uzticamam mākslīgajam intelektam"[418], kas sniedz ieteikumus ES iestādēm un dalībvalstīm, kā attīstīt, ieviest un veicināt mākslīgā intelekta izmantošanu un konkurētspēju Eiropā.

2020. gada 17. jūlijā AI HLEG pēc plašas sabiedriskās apspriešanas, diskusijām Eiropas Mākslīgā intelekta aliansē, kā arī izmēģināšanas procesa, kurā piedalījās vairāk nekā 350 organizācijas, publicēja Uzticama mākslīgā intelekta novērtēšanas saraksta gala versiju – praktisku rīku, lai palīdzētu uzņēmumiem un organizācijām pašām novērtēt to izstrādāto mākslīgā intelekta sistēmu atbilstību MI ētikas vadlīnijās noteiktajām septiņām uzticama mākslīgā intelekta prasībām.[419] Tas ir izstrādāts, stingri balstoties uz cilvēku pamattiesību aizsardzību. Dokumentā ir uzsvērts, ka ir jānovērtē mākslīgā intelekta sistēmu ietekme uz tādām pamattiesībām kā cilvēka cieņa, diskriminācijas aizliegums, tiesības uz privātumu un datu aizsardzību. Datu pārvaldības prasība paredz novērtēt datu aizsardzības noteikumu, kas izriet no VDAR, ievērošanu, piemēram, vai ir veikts novērtējuma par ietekmi uz datu aizsardzību, vai ir iecelts datu aizsardzības speciālists, vai pastāv uzraudzības mehānisms pār datu apstrādi, vai ir īstenoti pasākumi, lai nodrošinātu privātumu pēc noklusējuma un integrētu datu aizsardzību, minimizēšanas principa ievērošanu, vai, izstrādājot mākslīgā intelekta sistēmas, ir izmantotas tiesības atsaukt piekrišanu, tiesības iebilst un tiesības tikt aizmirstam.

Lai gan daudzas MI ētikas vadlīnijās ietvertās prasības izriet no spēkā esošām pamattiesībām, kā arī citiem tiesību aktiem, tajā pašā laikā tās nav juridiski saistošas. Turklāt tajās ir ietverta tikai daļa no VDAR izrietošajām prasībām.

417 European Commission. (2019). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Building Trust in Human Centric Artificial Intelligence. https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence

418 AI HLEG. (2019). Policy and investment recommendations for trustworthy Artificial Intelligence. https://www.europarl.europa.eu/italy/resource/static/files/import/intelligenza_artificiale_30_aprile/ai-hleg_policy-and-investment-recommendations.pdf

419 AI HLEG. (2020). Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment. https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

Eiropas Komisija 2020. gada 19. februārī publicēja Balto grāmatu par mākslīgo intelektu[420], kurā izklāstīti iespējamie mākslīgā intelekta tiesiskā regulējuma attīstības virzieni. Tā iepazīstina ar mākslīgā intelekta attīstības redzējumu, kas balstās uz izcilību un uzticēšanos. Tā apstiprina, ka ir jāīsteno un sinerģiski jāintegrē divi paralēli mākslīgā intelekta politikas mērķi. No vienas puses, jāveicina mākslīgā intelekta izpēte un ieviešana, lai ES būtu konkurētspējīga ar ASV un Ķīnu. Jācenšas mobilizēt resursus, lai panāktu "izcilības ekosistēmu", kas radītu pareizos stimulus, lai paātrinātu ekonomisko attīstību un lai Eiropa būtu piemērota digitālajam laikmetam un pozicionētos kā pasaules līdere ilgtspējīgu tehnoloģisko inovāciju jomā. No otras puses, mākslīgā intelekta tehnoloģiju ieviešanai būtu jāatbilst ES pamattiesībām un sociālajām vērtībām, radot uzticību. Kā norāda politoloģijas profesors Džovanni Sartors (*Giovanni Sartor*), ir svarīgi uzsvērt, ka abi mērķi ir savienojami, bet atšķirīgi. No vienas puses, visprogresīvākās mākslīgā intelekta lietojumprogrammas varētu izmantot, kaitējot pilsoņu tiesībām un sociālajām vērtībām. No otras puses, efektīva pilsoņu aizsardzība pret riskiem, ko rada mākslīgā intelekta ļaunprātīga izmantošana, pati par sevi nenodrošina stimulus, kas vajadzīgi, lai veicinātu pētniecību un inovāciju un lietderīgu mākslīgā intelekta izmantošanu.[421]

Lai radītu uzticēšanos mākslīgajam intelektam, ir jānodrošina tā atbilstība ES tiesiskajam regulējumam, ieskaitot pamattiesību un patērētāju tiesību regulējumu, it sevišķi attiecībā uz mākslīgā intelekta sistēmām, kas darbojas ES un rada augstu risku jeb bīstamību. Mākslīgā intelekta sistēmu izmantošana būtiskākos riskus rada tādu noteikumu piemērošanai, kuru mērķis ir aizsargāt pamattiesības, ieskaitot personas datu un privātuma aizsardzību, diskriminācijas aizlieguma principu, tiesības uz efektīvu tiesisko aizsardzību, kā arī patērētāju aizsardzību.

Baltā grāmata mudina izstrādāt jaunu mākslīgā intelekta tiesisko regulējumu un pieņemt juridiski saistošas prasības gadījumos, kad mākslīgā intelekta izmantošana rada augstu risku. Šis risks ir izsverams, izvērtējot, vai nozare un paredzētais izmantošanas veids nes līdzi būtisku apdraudējumu, sevišķi drošības, patērētāja tiesību un pamattiesību aizsardzības aspektā. Turklāt atsevišķos izņēmuma gadījumos mākslīgā intelekta izmantošana konkrētiem mērķiem pati par sevi ir uzskatāma par stipri bīstamu neatkarīgi no nozares. Viens no šādiem gadījumiem, kad mākslīgā intelekta izmantošana rada augstu risku, ir "biometriska attālināta identifikācija un citas uzbāzīgas novērošanas tehnoloģijas". Baltajā grāmatā ir norādīts, ka attiecībā uz mākslīgā intelekta izmantošanu, kas rada augstu risku, tiesiskajā regulējumā nosakāmās prasības varētu attiekties uz apmācību

420 Eiropas Komisija (2020), Baltā grāmata par mākslīgo intelektu.

421 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

datiem, datu un uzskaites glabāšanu, sniedzamo informāciju, noturību un precizitāti, cilvēka virsvadību, kā arī varētu tikt paredzētas īpašas prasības dažiem mākslīgā intelekta izmantošanas veidiem, piemēram, biometriskajai attālinātajai identifikācijai.

Līdzās pamattiesībām mākslīgais intelekts rada arī jautājumus, kā garantēt tā drošumu un tiesisko atbildību. Baltajai grāmatai par mākslīgo intelektu ir pievienots Ziņojums par mākslīgo intelektu, lietu internetu un robotiku drošuma un atbildības aspektā[422], kurā tiek analizēts spēkā esošais tiesiskais regulējums, lai novērtētu, vai un cik daudz pašreizējais regulējums par drošību un atbildību joprojām ir piemērots lietotāju aizsardzībai. Tas ir izstrādāts, balstoties uz Ekspertu grupas atbildības un jauno tehnoloģiju jomā 2019. gada novembrī publicēto Ziņojumu par mākslīgā intelekta un citu jauno tehnoloģiju atbildību, un sniedz ieteikumus par to, kā būtu jāizstrādā vai jāatjaunina atbildības režīmi ES, lai risinātu problēmas, kas izriet no straujajām tehnoloģiju izmaiņām.[423]

2020. gada 23. jūlijā Eiropas Komisija publicēja Sākotnējo ietekmes novērtējumu Priekšlikumam Eiropas Parlamenta un Padomes tiesību aktam, ar ko nosaka prasības mākslīgajam intelektam.[424] Tas papildina Balto grāmatu par mākslīgo intelektu, turpinot izvērtēt attiecīgās politikas iespējas un politikas instrumentus.

2020. gada 20. oktobrī Eiropas Parlaments pieņēma priekšlikumus par ES mākslīgā intelekta regulējuma izveidi attiecībā uz mākslīgā intelekta ētiku, atbildību par mākslīgā intelekta radīto kaitējumu un intelektuālā īpašuma tiesībām. Eiropas Parlaments rezolūcijā ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru mudina Eiropas Komisiju iesniegt jaunu tiesisko regulējumu un piedāvā priekšlikuma tekstu Regulai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrādes, ieviešanas un izmantošanas ētikas principiem.[425]

Eiropas Parlamenta piedāvātajā mākslīgā intelekta regulas priekšlikumā kā mērķis tika noteikts izveidot visaptverošu un nākotnes prasībām atbilstošu ES ētikas principu un juridisko pienākumu tiesisko regulējumu, saskaņā ar kuru ES

422 Eiropas Komisija. (2020). Komisijas ziņojums Parlamentam, Padomei un Eiropas Ekonomikas un sociālo lietu komitejai. Ziņojums par mākslīgo intelektu, lietu internetu un robotiku drošuma un atbildības aspektā. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020DC0064&from=en

423 European Commission. Expert Group on Liability and New Technologies – New Technologies Formation. (2019). Liability for Artificial Intelligence and Other Emerging Digital Technologies. https://op.europa.eu/publication/manifestation_identifier/PUB_DS0319853ENN

424 European Commission. (2020). Inception Impact Assessment. Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Requirements-for-Artificial-Intelligence

425 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

tiktu īstenota mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrāde, ieviešana un izmantošana (1. pants). Tajā tika noteikti vairāki būtiski principi, tostarp:

- uz cilvēku orientēts, cilvēku radīts un cilvēku kontrolēts mākslīgais intelekts, robotika un saistītās tehnoloģijas;
- obligāta augsta riska mākslīgā intelekta, robotikas un saistīto tehnoloģiju atbilstības novērtēšana;
- drošība, pārredzamība un pārskatatbildība;
- aizspriedumu un diskriminācijas nepieļaušana;
- tiesības uz tiesisko aizsardzību;
- sociālā atbildība un dzimumu vienlīdzība;
- vides ilgtspēja, privātās dzīves neaizskaramība un personas datu aizsardzība;
- biometriskās atpazīšanas izmantošanas ierobežojumi, laba pārvaldība.

Pirmajā nodaļā tika iekļauti vispārīgie noteikumi, kas paredz regulas pieņemšanas nolūku (1. pants), piemērošanas jomu (2., 3. pants), definīcijas (4. pants), kā arī vispārīgus noteikumus par ētikas principiem (5. pants). Otrajā nodaļā tika noteikti pienākumi attiecībā uz augsta riska tehnoloģijām, nosakot iepriekš minētos ētikas principus, pienākumu veikt riska novērtējumu (14. pants), atbilstības novērtēšanu (15. pants), kā arī paredzēti noteikumi attiecībā uz Eiropas ētiskās atbildības sertifikātu (16. pants). Tas paredzēja it īpaši regulēt augsta riska tehnoloģijas. Priekšlikuma pielikumā tika ietverts izsmeļošs un kumulatīvs augsta riska nozaru un augsta riska izmantošanas veidu un mērķu saraksts. Trešā nodaļa ietvēra institucionālās pārraudzības noteikumus, cita starpā nosakot pienākumu nodrošināt mākslīgā intelekta atbilstību pārvaldības standartiem, to skaitā attiecībā uz datiem, piemēram, veicot ārējo datu kvalitātes pārbaudes (17. pants), neatkarīgas uzraudzības iestādes izveidi katrā dalībvalstī (18. pants), kā arī ziņošanu par pārkāpumiem un ziņojošo personu aizsardzību (19. pants).

Eiropas Parlamenta piedāvātajā regulas priekšlikumā tika ietverti vispārīgi noteikumi par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētikas principiem, uzsverot vispārīgo pienākumu ikvienā gadījumā ievērot ES tiesību aktus un Hartā noteiktās pamattiesības (5. pants). Pirmkārt, tajā tika uzsvērts, ka jebkurš mākslīgais intelekts, robotika un saistītās tehnoloģijas, tostarp programmatūras, algoritmi un šādu tehnoloģiju izmantotie vai ģenerētie dati, ES ir jāizstrādā, jāievieš un jāizmanto saskaņā ar ES tiesību aktiem un pilnībā ievērojot cilvēka cieņu, autonomiju un drošību un citas Hartā noteiktas pamattiesības (5. panta 1. punkts). Otrkārt, tika akcentēts, ka tādu personas datu apstrādi, kas ir iegūti, izstrādājot, ieviešot un izmantojot mākslīgo intelektu, robotiku un saistītās tehnoloģijas, tostarp tādu personas datu apstrādi, kuru avots ir nepersonas dati un biometriskie dati, veic saskaņā ar VDAR un E-privātuma direktīvu. ES izstrādātam, ieviestam un izmantotam mākslīgajam intelektam, robotikai un saistītajām tehnoloģijām, tostarp programmatūrai, algoritmiem un šādu tehnoloģiju

izmantotiem vai ģenerētiem datiem, ir jābūt pilnīgā saskaņā ar ES pilsoņu tiesībām uz privātumu un personas datu aizsardzību (preambulas 35. punkts).

Priekšlikumā tika paredzētas prasības attiecībā uz biometriskās attālinātās atpazīšanas izmantošanu. Tajā tika noteikts privātās dzīves neaizskaramības un personas datu aizsardzības princips, kas paredz, ka biometrisko datu izmantošana un vākšana attālinātās identifikācijas nolūkos publiskās vietās, izmantojot biometrisko vai sejas atpazīšanu, īpaši apdraud pamattiesības, un to ievieš vai izmanto tikai dalībvalstu publiskās iestādes, aizstāvot būtiskas sabiedrības intereses. Minētās iestādes nodrošina, ka šādu pasākumu ieviešana vai izmantošana tiek darīta zināma sabiedrībai, ir samērīga, mērķtiecīga un aprobežojas ar konkrētiem mērķiem un atrašanās vietu un ir ierobežota laikā saskaņā ar ES un valstu tiesību aktiem, jo īpaši VDAR un E-privātuma direktīvu, un šajā ieviešanā un izmantošanā pienācīgi ņem vērā cilvēka cieņu un autonomiju, kā arī Hartā noteiktās pamattiesības, proti, tiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību (12. pants).

Tajā pašā laikā Eiropas Parlamenta regulas priekšlikums neparedzēja aizliegumus jeb sarkanās līnijas mākslīgā intelekta sejas atpazīšanas vai citu biometriskās attālinātās atpazīšanas sistēmu izmantošanai, kā arī cita veida mākslīgā intelekta novērošanas sistēmu izmantošanai. Tas neaizliedza tiesībaizsardzības iestādēm tās izmantot, atsaucoties uz sabiedrības vai valsts drošības interesēm, bet izvirzīja noteiktas prasības, atstājot tām rīcības brīvību izvērtēt atbilstību.

2021. gada 21. aprīlī Eiropas Komisija nāca klajā ar jaunu MI akta priekšlikumu[426], kas ir uzskatāms par ļoti nozīmīgu soli, jo tas ir pirmais priekšlikums pasaulē, kas paredz mākslīgā intelekta jomas tiesisko regulējumu. MI akta priekšlikums nosaka saskaņotus noteikumus mākslīgā intelekta sistēmu izmantošanai ES. Tas aizliedz noteiktus mākslīgā intelekta izmantošanas veidus, nosaka īpašas prasības augsta riska mākslīgā intelekta sistēmām, pārredzamības noteikumus mākslīgā intelekta sistēmām, kas paredzētas mijiedarbībai ar fiziskām personām, kā arī tirgus uzraudzības un mākslīgā intelekta sistēmu atbilstības uzraudzības noteikumus (1. pants).

Mākslīgā intelekta sistēmas ir paredzēts regulēt atkarībā no riska, ko tās rada, iedalot tās četrās dažādās riska kategorijas: mākslīgā intelekta sistēmas, kas rada minimālu risku, ierobežotu risku, augstu risku vai nepieņemamu risku.

MI akta priekšlikums paredz vairākus aizliegumus izmantot mākslīgā intelekta sistēmas, kuras uzskatāmas par nepieņemamām, jo ir pretrunā ar pamattiesībām un Eiropas vērtībām (5. pants). Pirmkārt, tas aizliedz praksi, kurai var būt ievērojams potenciāls manipulēt ar personām. Proti, ir aizliegta tādas mākslīgā intelekta sistēmas laišana tirgū, nodošana ekspluatācijā vai lietošana, kura

426 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

izmanto subliminālus paņēmienus, lai, personām to neapzinoties, būtiski iespaidotu personas uzvedību tādā veidā, kas šai vai citai personai rada vai var radīt fizisku vai psiholoģisku kaitējumu (5. panta 1. punkta a) apakšpunkts). Tāpat ir aizliegts izmantot noteiktu neaizsargātu grupu, piemēram, bērnu vai personu ar invaliditāti, neaizsargātības iezīmes, lai būtiski ietekmētu šai grupai piederīgas personas uzvedību tā, ka šai vai citai personai tiek vai var tikt radīts fizisks vai psiholoģisks kaitējums, piemēram, rotaļlietas-virtuālos palīgus, kas mudina bērnus uz bīstamu rīcību (5. panta 1. punkta b) apakšpunkts).

MI akta priekšlikums aizliedz sistēmas, kas ļauj valsts iestādēm veikt "sociālo novērtēšanu" vispārējiem mērķiem. Proti, ir aizliegta tādu mākslīgā intelekta sistēmu laišana tirgū, nodošana ekspluatācijā vai lietošana, ko veic publiskā sektora iestādes vai to vārdā fiziskas personas, lai izvērtētu vai klasificētu fizisku personu uzticamību noteiktā laikposmā, pamatojoties uz viņu sociālo uzvedību vai zināmām vai prognozētām personas vai personības īpašībām, ja sociālais novērtējums ved pie viena vai abiem šādiem iznākumiem (5. panta 1. punkta c) apakšpunkts). Šāda sociālā novērtēšanas sistēma pastāv Ķīnā, kur valsts vara ir ieviesusi plašu mākslīgā intelekta novērošanas sistēmu, kopā ar tā saukto sociālo kredīta sistēmu, lai kontrolētu iedzīvotājus, kas darbojas pretrunā ar demokrātiskām vērtībām.

Priekšlikums paredz aizliegt izmantot tiesībaizsardzības nolūkos reāllaika biometriskās attālinātās identifikācijas sistēmas sabiedriskās vietās (5. panta 1. punkta d) apakšpunkts). Tajā pašā laikā ir paredzēti arī vairāki izņēmuma gadījumi, kad šāda izmantošana ir atļauta, piemēram, ja tas ir nepieciešams smagu noziedzīgu nodarījumu atklāšanai. Visas pārējās fizisko personu attālinātās biometriskās identifikācijas sistēmas, ko izmanto valsts iestādes citos nolūkos vai privātie uzņēmumi, ir uzskatāmas par augsta riska sistēmām.

Cilvēktiesību aizstāvības organizācijas šiem noteikumiem ir veltījušas plašu kritiku.[427] Eiropas Datu aizsardzības uzraudzītājs vērš uzmanību, ka sarkanās līnijas būtu jānosaka stingrāk un jāaizliedz arī citas augsta riska biometriskās atpazīšanas sistēmas, piemēram, emociju uztveršanas sistēmas.[428]

MI akta priekšlikums paredz īpašus noteikumus mākslīgā intelekta sistēmām, kas rada augstu risku saskaņā ar 6. pantu, kā arī III pielikumu, kurā ir uzskaitītas daudzas jomas, kurās mākslīgā intelekta sistēmas uzskatāmas par augsta riska sistēmām. Šajā kategorijā cita starpā ietilpst fizisku personu biometriskā

427 EDRi. EU's AI law needs major changes to prevent discrimination and mass surveillance. https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/

428 EDPS. (23 April, 2021). Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary. https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en

identifikācija un kategorizācija, t. i. mākslīgā intelekta sistēmas, ko paredzēts izmantot fizisku personu attālinātai identifikācijai reāllaikā un vēlāklaikā. Augstu risku rada arī mākslīgā intelekta sistēmas, ko paredzēts izmantot tiesībaizsardzības iestādēs:

- sistēmas, kas paredzētas, lai veiktu individuālus riska novērtējumus, kuros vērtē risku, ka fiziska persona izdarīs pārkāpumu vai atkārtotu pārkāpumu, vai risku, kam pakļauti iespējamie noziedzīgos nodarījumos cietušie;
- sistēmas, ko paredzēts izmantot kā melu detektorus vai līdzīgus rīkus vai nolūkā noteikt fiziskas personas emocionālo stāvokli;
- mākslīgā intelekta sistēmas, ko paredzēts izmantot faktiska vai potenciāla noziedzīga nodarījuma izdarīšanas vai atkārtošanas prognozēšanai, pamatojoties uz fizisku personu profilēšanu vai fizisku personu vai grupu personības un rakstura īpašību vai agrākas noziedzīgas rīcības novērtēšanu;
- mākslīgā intelekta sistēmas, ko paredzēts izmantot fizisku personu profilēšanai noziedzīgu nodarījumu atklāšanas, izmeklēšanas vai kriminālvajāšanas gaitā;
- sistēmas, ko paredzēts izmantot noziegumu analīzei attiecībā uz fiziskām personām un kas ļauj tiesībaizsardzības iestādēm veikt meklēšanu lielās, kompleksās saistītu un nesaistītu datu kopās, kuras pieejamas dažādos datu avotos vai dažādos datu formātos, lai datos atklātu nezināmus modeļus vai slēptas sakarības.

Augstu risku rada arī mākslīgā intelekta izmantošana daudzās citās jomās, piemēram, migrācijas, patvēruma un robežkontroles pārvaldības jomā.

Augsta riska mākslīgā intelekta sistēmām ir piemērojamas stingras prasības. MI akta priekšlikums paredz pienākumu ieviest riska novērtēšanas sistēmu, lai noteiktu zināmus un paredzamus mākslīgā intelekta riskus, kā arī to samazināšanas un uzraudzības pasākumus. Attiecībā uz augsta riska mākslīgā intelekta sistēmām ir noteiktas prasības, kas attiecas uz izmantoto datu kopu kvalitāti, tehnisko dokumentāciju un uzskaiti, pārredzamību un informācijas sniegšanu lietotājiem, cilvēka virsvadību un noturību, precizitāti un kiberdrošību.

Regulas priekšlikums paredz arī detalizētus noteikumus par to, kā tiks uzraudzīta MI sistēmu atbilstība gan ES, gan valsts līmenī. Ir paredzēts izveidot Eiropas Mākslīgā intelekta padomi, un arī Latvijā būs jānozīmē atbildīgā uzraudzības institūcija. Eiropas līmenī tiks izveidota augsta riska mākslīgā intelekta sistēmu datubāze.

Mēs šobrīd nedzīvojam "tiesiskā vakuumā". Jaunais mākslīgā intelekta regulējums mēģina novērst trūkumus esošajā regulējumā. Jau šobrīd mākslīgā intelekta sistēmas regulē daudzi spēkā esošie tiesību akti, īpaši cilvēktiesību regulējums un datu aizsardzības noteikumi. Regulas horizontālā pieeja prasa nodrošināt tās

pilnīgu atbilstību spēkā esošajam ES tiesiskajam regulējumam attiecībā uz sektoriem, kuros tiek izmantotas augsta riska mākslīgā intelekta sistēmas.

Līdz šim diskusijas par mākslīgā intelekta regulējumu dziļi balstījās ES digitālā vienotā tirgus programmā, un, kaut arī tās var atsaukties uz nepieciešamību ņemt vērā tiesībaizsardzības un krimināltiesiskās īpatnības, šādas politikas diskusijas visbiežāk nav balstītas uz detalizētu šo jomu pārskatu un neņem vērā konkrētus piemērojamos noteikumus, it īpaši ierobežojumus un atkāpes.[429]

Tajā pašā laikā gan starptautiskā, gan ES līmenī arvien skaidrāk tiek pieprasīts skaidrs tiesiskais regulējums, kas noteiktu ierobežojumus, aizsardzības garantijas un prasības, to skaitā arī sarkanās līnijas attiecībā uz mākslīgā intelekta novērošanas tehnoloģiju izmantošanu.

Kā tika atklāts iepriekš, starptautiskās organizācijas – Eiropas Padome un ANO – jau ilgstoši ir mudinājušas pārskatīt starptautisko, kā arī nacionālo regulējumu, stiprināt datu aizsardzības standartus un nodrošināt efektīvas aizsardzības garantijas attiecībā uz masveida digitālās novērošanas pasākumiem. Sniegtie ieteikumi ir lielā mērā piemērojami arī attiecībā uz mākslīgā intelekta novērošanas tehnoloģijām. Daudzi no priekšlikumiem, kas sniegti iepriekš attiecībā uz digitālās novērošanas pasākumu regulējumu, šobrīd ir atrodami mākslīgā intelekta vadlīnijās, piemēram, nepieciešamība ievērot samērīguma principu, nodrošināt pārredzamību un atbildību. ES līmenī vislielākie nopelni masveida novērošanas ierobežošanā ir EST, kuras lēmumi ir vairākkārt likuši pārskatīt spēkā esošo regulējumu. Nākamajā nodaļā detalizētāk atklāts, kādas prasības cilvēktiesību ierobežošanai, piemērojot masveida novērošanas pasākumus, paredz starptautiskais cilvēktiesību regulējums un pārnacionālo tiesu – EST un ECT – izveidotā prakse. Atklāts, ka abas tiesas ir izstrādājušas būtiskas prasības, kas piemērojamas attiecībā arī uz mākslīgā intelekta tehnoloģijām un var palīdzēt nodrošināt to ētisku un atbildīgu izmantošanu, izvērtēt to samērīgumu un nepieciešamību, kā arī noteikt novērošanas tehnoloģiju izmantošanas robežas.

429 Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights.

5. DAĻA

Tiesību uz privātumu un datu aizsardzību ierobežošana: Eiropas tiesu prakse masveida novērošanas lietās

Izmantojot mākslīgā intelekta sistēmas, ir jāievēro cilvēktiesības, īpaši tiesības uz privātumu un datu aizsardzību. Mākslīgā intelekta, kā arī citi masveida novērošanas pasākumi būtiski apdraud cilvēktiesības. Tāpēc jautājums ir, kā noteikt robežas, cik tālu valsts var īstenot šādus pasākums, un kādi nosacījumi un garantijas ir jāievēro, lai cilvēktiesību ierobežojumi būtu samērīgi un likumīgi. Uz šo jautājumu ilgstoši ir centušās atbildēt divas Eiropas pārnacionālās tiesas – EST un ECT, izveidojot plašu tiesu praksi masveida novērošanas lietās. Šo tiesu nolēmumi, kuros ir analizēti cilvēktiesību ierobežošanas nosacījumi un nepieciešamās aizsardzības garantijas, kas ir jāpiemēro masveida novērošanas pasākumiem, ir svarīgs avots, lai varētu izvērtēt, vai valstu prakse nepārkāpj cilvēktiesības, arī gadījumos, kad tiek ieviesti un īstenoti mākslīgā intelekta novērošanas pasākumi.

Grāmatas turpinājumā vispirms sniegts ieskats, kādi ir cilvēktiesību dokumentos noteiktie tiesību uz privātumu un datu aizsardzību ierobežošanas nosacījumi. Pēc tam nodaļā aplūkots, kā šos nosacījumus ir piemērojusi ECT un EST masveida novērošanas lietās – kādas prasības un aizsardzības garantijas tās ir atzinušas par būtiskām, un kā tās būtu piemērojamas mākslīgā intelekta novērošanas tehnoloģijām, lai to ieviešana un izmantošana nepārkāptu tiesības uz privātumu un datu aizsardzību.[430]

5.1. Tiesību uz privātumu un datu aizsardzību ierobežošanas nosacījumi

Pastāv absolūtas cilvēktiesības, kuras nekādā gadījumā nevar ierobežot, piemēram, tiesības uz dzīvību. Tomēr lielāko daļu cilvēktiesību, tostarp tiesības uz privātumu un tiesības uz datu aizsardzību, var ierobežot. Tomēr šāda ierobežošana ir pieļaujama, tikai ievērojot konkrētus nosacījumus jeb ierobežošanas kritērijus.

Cilvēktiesību ierobežojumu kritēriji ir noteikti cilvēktiesību dokumentos. Gadījumi, kādos valsts var ierobežot tiesības uz privāto dzīvi, ir noteikti ECTK 8. panta 2. punktā: "Publiskās institūcijas nedrīkst traucēt nevienam baudīt šīs tiesības, izņemot gadījumus, kas ir paredzēti likumā un ir nepieciešami demokrātiskā sabiedrībā, lai aizsargātu valsts vai sabiedrisko drošību vai valsts

430 Grāmatā aplūkoti spriedumi, kurus EST un ECT ir pieņēmusi līdz 2021. gada aprīlim.

ekonomiskās labklājības intereses, lai nepieļautu nekārtības vai noziegumus, lai aizsargātu veselību vai tikumību, vai lai aizstāvētu citu tiesības un brīvības."

Saskaņā ar minēto normu tādas intereses kā valsts un sabiedriskā drošība, kā arī veselības aizsardzība ir pamats, lai varētu ierobežot cilvēktiesības. Tomēr šādi ierobežojumi ir pieļaujami tikai tad, ja tie ir "paredzēti likumā" un ir "nepieciešami demokrātiskā sabiedrībā", lai aizsargātu kādu no leģitīmajiem mērķiem. Pēdējais nosacījums arī paredz, ka iejaukšanās tiesībās ir jābūt proporcionālai izvirzītajam mērķim un ka šī mērķa sasniegšanai jāizraugās vismazāk ierobežojošais līdzeklis.[431]

Minētie cilvēktiesību ierobežošanas nosacījumi ir atrodami arī citos cilvēktiesību dokumentos. Hartas 7. un 8. pantā noteiktās tiesības uz privātumu un datu aizsardzību var ierobežot, ievērojot tiesību un brīvību ierobežošanas kritērijus. Šie kritēriji ir paredzēti Hartas 52. panta 1. punktā, kas nosaka: "Visiem šajā Hartā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jābūt noteiktiem tiesību aktos, un tajos jārespektē šo tiesību un brīvību būtība. Ievērojot proporcionalitātes principu, ierobežojumus drīkst uzlikt tikai tad, ja tie ir nepieciešami un patiešām atbilst vispārējas nozīmes mērķiem, ko atzinusi Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības."

Saskaņā ar minēto normu tiesību un brīvību izmantošanas ierobežojumiem ir jāatbilst pieciem kritērijiem, proti, tiem ir

1) jābūt noteiktiem tiesību aktos;
2) jārespektē tiesību un brīvību būtība;
3) jāatbilst vispārējas nozīmes mērķiem, ko atzinusi ES, vai vajadzībai aizsargāt citu personu tiesības un brīvības;
4) jābūt nepieciešamiem;
5) jābūt samērīgiem.

Hartā ietvertās tiesības atbilst ECTK garantētajām tiesībām, un šo tiesību nozīme un apjoms ir tāds pats kā ECTK noteiktajām tiesībām, kā to paredz Hartas 52. panta 3. punkts. Tajā pašā laikā minētā norma arī nosaka, ka tas neliedz ES tiesībās paredzēt plašāku aizsardzību. EST ir atzinusi, ka Hartas 52. panta 3. punkta mērķis ir nodrošināt nepieciešamo saskaņotību starp tajā ietvertajām tiesībām un atbilstošajām ECTK garantētajām tiesībām, tomēr negatīvi neietekmējot ES tiesību un EST autonomiju. Interpretējot Hartu, kā minimālās aizsardzības robeža ir jāņem vērā atbilstošās ECTK tiesības.[432] Cilvēktiesību ierobežošanas nosacījumi, kas paredzēti ECTK 8. panta 2. punktā, kā tos ir piemērojusi ECT, ir minimālie nosacījumi, kas jāievēro, ierobežojot Hartā paredzētās tiesības uz privātumu. Izvērtējot ES tiesību aktu atbilstību vai interpretāciju saskaņā ar Hartu,

431 European Court of Human Rights (2020), Guide on Article 8 of the Convention.

432 Sk. EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 124. punkts.

EST ir jāņem vērā garantijas, kuras noteiktas ECT praksē, izvērtējot atbilstību ECTK. Tajā pašā laikā EST var paredzēt arī plašāku aizsardzību.

Cilvēktiesību dokumentos paredzētie cilvēktiesību ierobežošanas kritēriji nosaka vispārējo kārtību, kādā ir jāveic samērīguma pārbaude un jāizvērtē tiesību ierobežošanas likumība, kas ir jāņem vērā, arī ieviešot jaunus masveida novērošanas pasākumus, to skaitā izmantojot jaunās tehnoloģijas. Eiropas Datu aizsardzības uzraudzītājs 2019. gadā publicēja Vadlīnijas par pasākumiem, kuri ierobežo pamattiesības uz privātumu un personas datu aizsardzību, proporcionalitātes novērtēšanu. Vadlīnijas balstās uz EST praksi masveida novērošanas lietās un skaidro proporcionalitātes principa piemērošanu. Vadlīnijas piedāvā praktisku metodiku jaunu likumdošanas pasākumu samērīguma novērtēšanai politikas veidotājiem un likumdevējam.[433] Dokumentā ir uzsvērts, ka nosacījumi iespējamiem pamattiesību ierobežojumiem ir vieni no svarīgākajiem Hartas elementiem, jo tie paredz, cik lielā mērā pamattiesības var tikt efektīvi izmantotas.[434] Tālāk apskatīts, kādus nosacījumus pamattiesību ierobežošanai ir noteikušas Eiropas pārnacionālās tiesas.

5.2. Nozīmīgākās masveida novērošanas lietas

ECT un EST ir izskatījusi un turpina izskatīt daudzas masveida novērošanas lietas.[435] ECT izskata sūdzības pret valstu novērošanas pasākumiem. Savukārt EST ir izskatījusi daudzas novērošanas lietas, kuras saistītas ar ES tiesību aktu spēkā esamību vai interpretāciju un kurās jautājumus ir uzdevusi valstu nacionālā tiesa, lūdzot sniegt prejudiciālo nolēmumu, vai arī ES institūcija, lūdzot sniegt viedokli. Daudzas nacionālās tiesas, kā arī Eiropas pārnacionālās tiesas izskata arī kolektīvās sūdzības masveida novērošanas lietās. Kā nodaļā atklāts, vairākas nevalstiskās organizācijas, piemēram, "Big Brother Watch", kā arī atsevišķas personas, piemēram, Maksimilians Šrems, kopējo interešu vārdā ir ierosinājušas stratēģiskās tiesvedības, lai apstrīdētu masveida novērošanas pasākumus.[436]

433 EDPS. (2019). EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en

434 Ibid.

435 Council of Europe. (2018). Mass surveillance; European Court of Human Rights (2020), Guide on Article 8 of the Convention, p. 40.

436 Taylor, van der Sloot, Floridi (2017), Conclusion: What Do We Know About Group Privacy?, pp. 232, 233.

5.2.1. Eiropas Cilvēktiesību tiesas prakse

ECT masveida novērošanas tiesu prakse ir ļoti plaša.[437] ECT ir izskatījusi daudzas uzraudzības lietas par elektronisko sakaru pārtveršanu[438], dažādiem novērošanas veidiem gan valsts, gan privātajā sektorā[439] un personas datu glabāšanu, ko veic valsts iestādes.[440] ECT ir atzinusi, ka ECTK 8. pants attiecas ne tikai uz valsts veiktu elektronisko sakaru novērošanu, bet arī, piemēram, uz videonovērošanu sabiedriskās vietās, piemēram, universitātēs un lielveikalos. Tālāk nodaļā apskatītas dažas nozīmīgākās ECT lietas.

Saskaņā ar ECT judikatūru tas būtu pretrunā ar valdību centieniem apkarot terorismu, ja terorisma draudi tiktu aizstāti ar iespējamiem draudiem no neierobežotas izpildvaras, kas iejaucas pilsoņu privātajā dzīvē.[441] Viena no pirmajām lietām, kurā ECT pieņēma spriedumu jau 1978. gadā, bija "Klāss u. c. pret Vāciju".[442] Šajā lietā iesniedzēji – pieci vācu juristi – apstrīdēja Vācijas tiesību aktus, kas pilnvaroja iestādes novērot viņu saraksti un telefona sakarus, neuzliekot tām pienākumu viņus vēlāk informēt par šiem pasākumiem. ECT nekonstatēja ECTK 8. panta pārkāpumu, atzīstot, ka iejaukšanās bijusi samērīga. Tajā pašā laikā tā pauda vairākas būtiskas atziņas. ECT atzina, ka ECTK 8. pantā noteiktais privātās dzīves jēdziens attiecas uz telefona sarunu slepenu noklausīšanos.[443] Tālāk tā norādīja, ka valsts likumdevējam ir zināma rīcības brīvība noteikt nosacījumus, saskaņā ar kuriem novērošanas sistēma darbojas. Tomēr tas nenozīmē, ka valstīm ir neierobežota rīcības brīvība pakļaut slepenai novērošanai to jurisdikcijā esošās personas. Apzinoties, ka šāds likums var radīt draudus demokrātijai vai pat to graut un iznīcināt, un izvirzot mērķi demokrātiju aizsargāt, valstis nedrīkst veikt jebkāda veida pasākumus, ko tās uzskata par piemērotiem cīņai pret spiegošanu un terorismu. Neatkarīgi no tā, kāda ir novērošanas sistēma, jāpastāv pietiekamām un efektīvām garantijām pret tās ļaunprātīgu izmantošanu. ECT norādīja, ka to izvērtējumam ir relatīvs raksturs, kas atkarīgs no visiem lietas apstākļiem, piemēram, iespējamo pasākumu rakstura, apjoma un ilguma, pamatojuma, kas

437 Sk. Council of Europe. (2018). Mass Surveillance; European Court of Human Rights (2020), Guide on Article 8 of the Convention.

438 Sk., piemēram, ECT 1984. gada 2. augusta spriedums lietā 8691/79 *Malone v. the United Kingdom*; ECT 2007. gada 3. aprīļa spriedums lietā 62617/00 *Copland v. The United Kingdom*; ECT 2017. gada 18. jūlija spriedums lietā 27473/06 *Mustafa Sezgin Tanrıkulu v Turkey*.

439 Sk., piemēram, ECT 1978. gada 6. septembra spriedums lietā 5029/71 *Klass and Others v. Germany*; ECT 2010. gada 2. septembra spriedums lietā *Uzun v. Germany*.

440 Sk., piemēram, ECT 2015. gada 4. decembra spriedums lietā 47143/06 *Roman Zakharov v. Russia*; ECT 2016. gada 12. janvāra spriedums lietā 37138/14.

441 Sk. Council of Europe (2018), Mass Surveillance.

442 ECT 1978. gada 6. septembra spriedums lietā 5029/71.

443 Turpat, 41. punkts.

nepieciešams šādu pasākumu ieviešanai, iestādes, kas ir kompetenta atļaut, veikt un uzraudzīt šādus pasākumus, valsts tiesību aktos paredzēto tiesiskās aizsardzības līdzekļu veida.[444]

ECT lietā "Szabó un Vissy pret Ungāriju" izvērtēja Ungārijas tiesību aktus, kas paredz slepenu, ar pretterorismu saistītu novērošanu, kas veikta, izmantojot jaunās tehnoloģijas, un ļauj masveidā pārtvert elektronisko sakaru datus. Iesniedzējs apgalvoja, ka regulējums nebija pietiekami detalizēts, precīzs, kā arī tas nesniedza pietiekamas garantijas pret datu ļaunprātīgu izmantošanu un valsts iestāžu patvaļu.[445]

ECT atgādināja, ka ECTK 8. pantā noteiktais privātās dzīves jēdziens attiecas uz sakaru un telefona sarunu noklausīšanos, ko veic policija, izlūkdienesti vai citas tiesībaizsardzības iestādes. Turklāt ECT spriedumā uzmanība tika vērsta arī uz to, ka, ņemot vērā slepenās novērošanas pasākumu īpatnības un to efektīvas kontroles un uzraudzības nozīmi, noteiktos apstākļos persona var apgalvot, ka ir upuris, tikai tāpēc, ka pastāv tiesību akti, kas atļauj slepenu novērošanu, pat ja šī persona nevar norādīt uz kādiem konkrētiem pasākumiem, kas viņu tieši ietekmē. [446]

ECT arī vērsa uzmanību, ka valdību iespēja iegūt detalizētu pilsoņu dzīves intīmāko aspektu aprakstu var radīt īpaši ierobežojošu iejaukšanos privātajā dzīvē.[447] Jāatceras, ka, izmantojot tehnoloģijas, kas balstītas uz mākslīgo intelektu, var daudz vieglāk veikt personas datu sasaisti dažādās sistēmās un profilu apvienošanu.[448]

ECT lietā arī norādīja, ka moderno tehnoloģiju, tostarp masveida komunikāciju novērošanas, izmantošana, lai novērstu potenciālus uzbrukumus, ir dabiskas sekas mūsdienu terorisma veidiem, ar ko valstīm nākas saskarties. Tomēr ECT atzina, ka attiecīgie Ungārijas tiesību akti nenodrošina pietiekamus aizsardzības pasākumus, lai izvairītos no ļaunprātīgas izmantošanas. ECT vērsa uzmanību, ka pasākumi varētu skart praktiski ikvienu Ungārijas iedzīvotāju, un jaunās tehnoloģijas ļauj valdībai viegli pārtvert liela apjoma datus, kas attiecas pat uz personām, attiecībā uz kurām šādas darbības sākotnēji netika paredzēts veikt. ECT konstatēja pārkāpumu, norādot, ka šādus pasākumus uzraudzīja tikai izpildvara, neizvērtējot, vai saziņas pārtveršana ir noteikti nepieciešama, un nepastāvēja neatkarīga tiesas kontrole un efektīvi tiesību aizsardzības pasākumi.

444 ECT 1978. gada 6. septembra spriedums lietā 5029/71, 49.–50. punkts.

445 ECT 2016. gada 12. janvāra spriedums lietā 37138/14, 33. punkts.

446 Turpat, 53. punkts.

447 Turpat, 70. punkts.

448 Gonzelez Fuster (2020), Artificial Intelligence and Law Enforcement, p. 38.

Grāmatas rakstīšanas laikā 2020. gada beigās ECT izskatīšanā atradās vairākas lietas par masveida komunikācijas datu novērošanu. 2019. gadā ECT paziņoja, ka tā atkārtoti izskatīs "Big Brother Watch u. c. pret Apvienoto Karalisti"[449] un "Centrum för Rättvisa pret Zviedriju"[450] lietas Lielajā palātā. 2018. gadā abās lietās ECT atzina, ka masveida novērošanas režīmi, lai gan aizskar tiesības uz privātumu, ir pieļaujami un paši par sevi nepārkāpj ECTK. Tāpat ECT uzsvēra, ka metadatu pārtveršana var būt tikpat aizskaroša, kā satura datu iegūšana. Tajā pašā laikā tā sniedza kritēriju sarakstu, kas jāņem vērā, izvērtējot pasākuma likumību, nepieciešamību un samērīgumu.

2018. gada 13. septembra spriedumā lietā "Big Brother Watch u. c. pret Apvienoto Karalisti" ECT konstatēja, ka Apvienotās Karalistes slepenās novērošanas programma pārkāpa ECTK 8. pantā noteiktās pamattiesības uz privātās dzīves ievērošanu nepietiekamas neatkarīgas uzraudzības un nepietiekamu aizsardzības pasākumu dēļ. Lieta attiecās uz žurnālistu un cilvēktiesību aizstāvju organizācijas sūdzību par trim dažādiem novērošanas režīmiem:

1) liela apjoma sakaru pārtveršanu;
2) sakaru datu iegūšanu, ko veica sakaru pakalpojumu sniedzēji, un
3) izlūkošanas informācijas apmaiņu ar ārvalstu valdībām.

ECT konstatēja pārkāpumus saistībā ar pirmajiem diviem gadījumiem. Tā vērsa uzmanību, ka pirmajā gadījumā nepastāvēja pietiekama uzraudzība pār pasākuma piemērošanu, bet otrajā gadījumā pasākums nebija skaidri noteikts likumā.[451] Šajā lietā ECT konstatēja, ka bija arī pārkāptas tiesības uz vārda brīvību, kas noteiktas ECTK 10. pantā, jo nepastāvēja pietiekami drošības pasākumi attiecībā uz konfidenciāliem žurnālistikas materiāliem.[452]

Savukārt 2018. gada 19. jūnija spriedumā lietā "Centrum för Rättvisa pret Zviedriju" ECT konstatēja, ka Zviedrijas lielapjoma sakaru pārtveršanas sistēma sniedz pietiekamas garantijas pret patvaļu un ļaunprātīgas izmantošanas risku. ECT norādīja šādus kritērijus, kas ļāva konstatēt pasākumu atbilstību: signālu izlūkošanas pasākumu darbības joma un pārtverto datu apstrāde bija skaidri noteikta likumā; atļaujai pārtvert datus vajadzēja būt ar tiesas lēmumu pēc detalizētas pārbaudes; pārtvert bija atļauts tikai sakarus, kas šķērso Zviedrijas robežu, bet ne pašā Zviedrijā; pārtveršana var ilgt tikai sešus mēnešus; jebkura atjaunošana prasīja pārskatīšanu; bija vairākas neatkarīgas struktūras, it īpaši Ārējās izlūkošanas inspekcija, kuras uzdevums bija uzraudzīt un pārskatīt sistēmu;

449 ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13, 62322/14, 24960/15 *Big Brother Watch and Others v. The United Kingdom.*

450 ECT 2018. gada 19. jūnija spriedums lietā 35252/08 *Centrum för Rättvisa v. Sweden.*

451 ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13 .., 387., 388. punkts.

452 Turpat, 495. punkts.

novērošanas pasākumu nepaziņošanu kompensēja fakts, ka bija pieejami vairāki sūdzību iesniegšanas mehānismi, it īpaši vēršoties pie Ārējās izlūkošanas inspekcijas, Parlamentārā ombuda un Tieslietu kanclera.[453]

ECT ir atzinusi, ka valstīm nav neierobežotas pilnvaras veikt iedzīvotāju masveida novērošanu. Saskaņā ar ECT praksi šāda novērošana ir pieļaujama tikai tad, ja tā ir absolūti nepieciešama demokrātisku mērķu aizsardzībai. Ņemot vērā lielo iespējamību, ka ECTK nostiprinātās pamattiesības uz privātumu un vārda brīvību var tikt pārkāptas, valstīm ir jānodrošina, ka, ieviešot novērošanas pasākumus, kas ietver masveida datu vākšanu, vienlaikus tiek izstrādāti arī tiesiski aizsardzības pasākumi, kas nodrošina cilvēktiesību ievērošanu.

Pamatkritērijiem, lai izvērtētu, vai masveida novērošanas pasākumi atbilst cilvēktiesībām, jābūt tikpat stingriem un saskaņotiem kā mērķtiecīgiem novērošanas pasākumiem.[454] Eiropas Padome ir norādījusi, ka ir ārkārtīgi svarīgi, lai valsts tiesību akti, kas atļauj aizskarošu novērošanas tehnoloģiju izmantošanu, paredz arī pietiekamas aizsardzības garantijas, lai novērstu vārda brīvības un tiesību uz privāto dzīvi riskus, kas rodas no milzīga datu apjoma masveida nediferencētas iegūšanas. Tāpēc ECT judikatūrā noteiktie standarti, kas saistīti ar mērķtiecīgu novērošanu, jāpielāgo arī masveida novērošanai.[455]

Lai gan ECT vēl nav skatījusi lietas par mākslīgā intelekta tehnoloģiju izmantošanas atbilstību cilvēktiesībām, tomēr tā ir paudusi viedokli par fotogrāfiju, kas glabājas policijas datubāzēs, izmantošanu sejas atpazīšanai. ECT 2020. gada 13. februārī pieņēma spriedumu lietā "Gaughran pret Apvienoto Karalisti" par notiesātas personas DNS profila, pirkstu nospiedumu un fotogrāfijas saglabāšanu.[456] Lietā cita starpā tika izskatīts jautājums par datubāzi, kurā glabātās fotogrāfijas var izmantot sejas atpazīšanas nolūkos, kas sākotnēji nebija iespējams, bet vēlāk kļuva iespējams, jo datus varēja pārsūtīt uz citu datubāzi, kuru varēja izmantot sejas atpazīšanai.[457] Proti, kopš 2016. gada jūlija Policijas nacionālajā datubāzē bija vairāk nekā 19 miljoni attēlu, no kuriem vairāk nekā 16 miljoni bija reģistrēti sejas atpazīšanas galerijā, padarot tos meklējamus, izmantojot sejas atpazīšanas programmatūru. ECT norādīja, ka iesniedzēja fotogrāfijas uzņemšana un saglabāšana nozīmē iejaukšanos viņa tiesībās uz privāto dzīvi ECTK 8. panta 1. punkta izpratnē, ņemot vērā to, ka fotogrāfija tika uzņemta viņa apcietināšanas laikā un

453 ECT 2018. gada 19. jūnija spriedums lietā 35252/08, 177., 178., 180. punkts.

454 Gstrein (2020), Mapping Power and Jurisdiction on the Internet ..

455 Council of Europe (2018), Mass Surveillance.

456 ECT 2020. gada 13. februāra spriedums lietā 45245/15 *Gaughran v. The United Kingdom.*

457 Turpat, 13., 37., 68., 69. punkts.

uz nenoteiktu laiku tiks glabāta vietējā datubāzē, lai to izmantotu policija, un ka policija var fotogrāfijai piemērot arī sejas atpazīšanu.[458]

ECT spriedumā nepārprotami tika noraidīts Apvienotās Karalistes valdības arguments – "jo vairāk dati tiek saglabāti, jo vairāk tiek novērsta noziedzība", norādot, ka "praksē šāda argumenta pieņemšana datu neierobežotas glabāšanas kontekstā būtu līdzvērtīga tam, ka tiktu atzīta par pieļaujamu informācijas glabāšana par visiem iedzīvotājiem un viņu mirušajiem radiniekiem, kas noteikti būtu pārmērīga un neatbilstoša".[459]

ECT arī vērsa uzmanību, ka ir jāizvērtē un jāpamato, kādos gadījumos un cik ilgu laiku dati ir jāglabā atkarībā, piemēram, no noziedzīgā nodarījuma smaguma, kā arī jānodrošina tiesību aizsardzības iespējas. ECT atzina, ka netiek nodrošināts līdzsvars starp konkurējošām valsts un personas interesēm, ņemot vērā prasītāja kā par pārkāpumu notiesātas personas (pat ja prasība tiek uzturēta) DNS profila, pirkstu nospiedumu un fotogrāfijas glabāšanas pilnvaru nediferencēto raksturu (šīs darbības veiktas neatkarīgi no nodarījuma smaguma vai nepieciešamības saglabāt datus nenoteiktu laiku) un reālu tiesību aizsardzības iespēju neesamību.

Visticamāk, šī lieta ir tikai sākums daudzām lietām, kuras nākotnē tiks iesniegtas par sejas atpazīšanas un citu mākslīgā intelekta sistēmu izmantošanu un kuras būs jāizskata gan ECT, gan EST.

5.2.2. Eiropas Savienības Tiesas prakse

EST daudzās lietās, kas saistītas ar masveida novērošanas pasākumiem, ir vērtējusi to atbilstību gan tiesībām uz privātumu, gan tiesībām uz datu aizsardzību. EST ir atzinusi, ka gadījumā, ja tiek ietekmētas Hartas 7. pantā noteiktās pamattiesības uz privātās dzīves neaizskaramību, apstrādājot personas datus, tiek ietekmētas arī tiesības uz datu aizsardzību, jo šāda apstrāde ietilpst Hartas 8. panta tvērumā un tai obligāti jāatbilst šajā pantā paredzētajām datu aizsardzības prasībām.[460] EST ir norādījusi, ka ES dalībvalstīm ar valsts tiesisko regulējumu noteiktais pienākums elektronisko komunikāciju pakalpojumu sniedzējiem saglabāt informāciju par datu plūsmu, lai to vajadzības gadījumā padarītu pieejamu kompetentajām valsts iestādēm, izraisa jautājumus ne tikai par privātās dzīves un personas datu aizsardzību, bet arī par Hartas 11. pantā garantēto vārda brīvību.

458 ECT 2020. gada 13. februāra spriedums lietā 45245/15 *Gaughran v. The United Kingdom*, 70. punkts

459 Turpat., 89. punkts.

460 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 170.–171. punkts.

Tas pats attiecas arī uz citiem datu apstrādes veidiem, piemēram, to nodošanu citām personām, kas nav lietotāji, vai piekļuvi šiem datiem, lai tos izmantotu.[461]

Personas datu izpaušana trešajai personai, piemēram, valsts iestādei, ir iejaukšanās Hartas 7. pantā un 8. pantā noteiktajās pamattiesībās, lai kāda būtu izpaustās informācijas tālākā izmantošana. Tas pats attiecas uz personas datu saglabāšanu, kā arī uz piekļuvi minētajiem datiem, lai valsts iestādes tos izmantotu neatkarīgi no tā, vai attiecīgajai informācijai par privāto dzīvi ir vai nav sensitīvs raksturs un vai ieinteresētajām personām ir vai nav radītas iespējamas neērtības šīs iejaukšanās dēļ.[462]

EST ir atzinusi – lai izpildītu samērīguma prasību, tiesiskajā regulējumā ir jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma tvērumu un piemērošanu un paredz minimālās prasības, lai tā rezultātā personām, kuru personas dati ir aizskarti, būtu pietiekamas garantijas, kas ļautu šos datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku. Tiesiskajā regulējumā it īpaši ir jānorāda, kādos apstākļos un ar kādiem nosacījumiem var īstenot pasākumus, kas ietver šādu datu apstrādi, tādējādi garantējot, ka iejaukšanās notiek tikai absolūti nepieciešamā robežās.[463] Līdz ar to valsts iestāžu piekļuve personas datiem, to saglabāšana un turpmāka izmantošana, īstenojot novērošanas pasākumus, nedrīkst pārsniegt robežas, kas ir absolūti nepieciešamas, citādi to "nevar uzskatīt par pamatotu demokrātiskā sabiedrībā".[464]

EST ir izskatījusi daudzas lietas, kas saistītas ar datu saglabāšanas pienākumu elektroniskās komunikācijas pakalpojumu sniedzējiem drošības iestāžu vajadzībām. Viena no būtiskajām lietām, kas īpaši nozīmīga privātuma un datu aizsardzības kā pamattiesību aizsardzības kontekstā, ir "Digital rights Ireland"[465] lieta, kurā EST pieņēma nolēmumu 2014. gadā. EST atzina šajā lietā par spēkā neesošu Datu saglabāšanas direktīvu, kas paredzēja elektroniskās komunikācijas pakalpojumu sniedzējiem pienākumu saglabāt datus un nodot tos drošības iestādēm pēc pieprasījuma. EST secināja, ka iejaukšanās pamattiesībās pārsniedz to, kas ir absolūti nepieciešams valsts drošības aizsardzībai, un tādējādi neatbilst Hartas 52. panta 1. punktā paredzētajam proporcionalitātes principam.

Pēc šī sprieduma EST izskatīja vēl vairākas lietas, kurās izvērtēja, vai ES tiesības pieļauj valstīs dažādus režīmus, kas paredz elektroniskās komunikācijas datu saglabāšanu nacionālajos tiesību aktos. 2016. gadā EST pieņēma nolēmumu

461 EST 2020. gada 6. oktobra spriedums lietā C-623/17 *Privacy International*, ECLI:EU:C:2020:790, 60.–61. punkts.

462 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 171. punkts.

463 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 68. punkts un tur minētā jurisprudence.

464 Turpat, 81. punkts.

465 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C293/12 ..

"Tele2 Sverige AB" un "Watson u. c."[466] apvienotajās lietās, atzīstot, ka E-privātuma direktīva neaizliedz dalībvalstīm pieņemt tiesību aktus, kas atvieglotu mērķtiecīgu (*targeted* – angļu val.) datu plūsmas un atrašanās vietas datu saglabāšanu smagu noziegumu apkarošanai, tajā pašā laikā tā aizliedz nacionālajās tiesībās paredzēt normas, kas uzliek elektronisko sakaru pakalpojumu sniedzējiem visaptverošu un nediferencētu datu saglabāšanas pienākumu.

Minētajā lietā EST arī atteicās no sava iepriekš paustā viedokļa, ka tiesību uz privātumu kontekstā komunikācijas saturs būtu vairāk aizsargājams nekā metadati. EST 2015. gada spriedumā "Schrems I" lietā norādīja, ka "it īpaši tiesiskais regulējums, saskaņā ar kuru valsts iestādēm vispārīgi tiek ļauts piekļūt elektronisko komunikāciju saturam, ir jāuzskata par tādu, kas apdraud pašu Hartas 7. pantā garantēto pamattiesību uz privātās dzīves neaizskaramību būtību".[467] Savukārt spriedumā "Tele 2 Sverige AB" un "Watson u. c." apvienotajās lietās, kā arī turpmākās lietās EST tomēr pamatoti atkāpās no šī apsvēruma, atzīstot, ka metadati kontekstā ar tiesībām uz privātās dzīves neaizskaramību var sniegt tikpat sensitīvu informāciju kā pats šīs komunikācijas saturs.[468] Dati, kuri tādējādi ir jāsaglabā elektronisko komunikāciju pakalpojumu sniedzējiem, ļauj atrast un identificēt saziņas avotu un tās adresātu, noteikt saziņas datumu, laiku, ilgumu un veidu, lietotāju izmantoto saziņas aparātu, kā arī noteikt mobilās saziņas aparāta atrašanās vietu. Šie dati ietver tostarp abonenta vai reģistrētā lietotāja vārdu un adresi, izsaucēja telefona numuru un zvana adresāta telefona numuru, kā arī IP adresi interneta pakalpojumiem. Šie dati it īpaši ļauj uzzināt, ar kuru personu abonents vai reģistrētais lietotājs ir sazinājies un kādu sakaru līdzekli viņš ir izmantojis, kā arī ļauj noteikt saziņas laiku un vietu, no kuras šī saziņa notikusi. Turklāt šie dati ļauj noskaidrot abonenta un reģistrēta lietotāja saziņas ar noteiktām personām biežumu noteiktā laikposmā.[469] Šie dati kopumā var ļaut izdarīt ļoti precīzus secinājumus par personu, kuru dati tikuši saglabāti, privāto dzīvi, proti, ikdienas paradumiem, pastāvīgajām vai pagaidu uzturēšanās vietām, ikdienas vai citām gaitām, veiktajām darbībām, šo personu sociālajiem kontaktiem un aprindām, kurās tās mēdz uzturēties. Šie dati sniedz iespējas noteikt attiecīgo personu profilu, kas kontekstā ar tiesībām uz privātās dzīves neaizskaramību ir tikpat sensitīva informācija kā pats šīs saziņas saturs.[470]

466 EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15 *Tele2 Sverige AB* un C-698/15 *Watson u. c.,* ECLI:EU:C:2016:970.

467 EST 2015. gada 6. oktobra spriedums lietā C-362/14, 94. punkts.

468 EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15 .., 98. punkts. Sk. arī EST 2014. gada 8. aprīļa spriedumu apvienotajās lietās C293/12 .., 26. punkts; EST 2020. gada 6. oktobra spriedumu apvienotajās lietās .., 117., 184. punkts.

469 EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15 .., 98. punkts.

470 Turpat, 99. punkts.

Vairākas ES dalībvalstis nepiekrita EST interpretācijai, ka ir aizliegta informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta glabāšana, jo uzskatīja, ka tām tiek atņemts būtisks instruments valsts drošības aizsargāšanai un cīņai pret terorismu. Šis pretējais viedoklis bija pamats vairākām jaunām EST prejudiciāla nolēmuma lūguma lietām par datu saglabāšanu, kurās apvienotais spriedums tika pasludināts 2020. gada 6. oktobrī – Francijas lietās C-511/18 "La Quadrature du Net u. c." un C-512/18 "French Data Network u. c." un Beļģijas lietā C-520/18 "Ordre des barreaux francophones et germanophone u. c."[471]

Atšķirībā no "Tele 2 Sverige AB" un "Watson u. c." lietām, kurās EST izvērtēja dalībvalstu regulējumu, kas paredzēja datu saglabāšanas pienākumu, lai apkarotu smagus noziegumus, jaunajās EST lietās jautājumi ir uzdoti par valsts drošības aizsardzību. EST tika jautāts, vai gadījumā, ja šādu pasākumu, kuri ierobežo tiesības uz privātumu un datu aizsardzību, mērķis ir valsts drošības garantēšana, interpretācija ir atšķirīga, t. i., vai E-privātuma direktīva ir piemērojama, un vai tomēr šādā gadījumā nebūtu pieļaujams paredzēt visaptverošu un nediferencētu datu saglabāšanas pienākumu.

Apvienotās Karalistes lietā "Privacy International" EST, atsaucoties uz savu iepriekšējo judikatūru, atgādināja, ka iejaukšanās Hartas 7. pantā paredzētajās tiesībās uz privātās dzīves neaizskaramību, ko rada informācijas par datu plūsmu un atrašanās vietas datu nodošana drošības dienestiem un izlūkdienestiem, ir jāuzskata par īpaši smagu, ņemot vērā tostarp informācijas, kuru var sniegt šie dati, sensitīvo raksturu un it īpaši iespēju, pamatojoties uz tiem, pierādīt datu subjekta profilu, jo šāda informācija ir tikpat sensitīva kā pats komunikācijas saturs. Turklāt šis apstāklis datu subjektu apziņā var radīt sajūtu, ka to privātā dzīve tiek pastāvīgi novērota.[472] Informācijas par datu plūsmu un atrašanās vietas datu nodošana valsts iestādēm drošības nolūkos pati par sevi var apdraudēt Hartas 7. pantā nostiprināto tiesību uz saziņas neaizskaramību. Tas elektroniskās komunikācijas līdzekļu izmantotājus var atturēt izmantot savu vārda brīvību, kas ir garantēta Hartas 11. pantā.[473] EST arī vērsa uzmanību, ka, ņemot vērā informācijas par datu plūsmu un atrašanās vietas datu, kurus var pastāvīgi saglabāt ar visaptverošu un nediferencētu saglabāšanas pasākumu, ievērojamo apjomu, kā arī informācijas, ko šie dati var sniegt, sensitīvo raksturu, pati minēto datu saglabāšana, ko veic elektronisko komunikāciju pakalpojumu sniedzēji, ietver ļaunprātīgas izmantošanas un

471 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 ..

472 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 71. punkts. Sk. arī EST 2014. gada 8. aprīļa spriedumu apvienotajās lietās C-293/12 **..**, 27. un 37. punkts, kā arī EST 2016. gada 21. decembra spriedumu apvienotajās lietās C-203/15 .., 99. un 100. punkts.

473 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 72. punkts.

prettiesiskas piekļuves risku.[474] Lai izpildītu samērīguma prasību, atkāpes no personas datu aizsardzības un tās ierobežojumi ir jāīsteno absolūti nepieciešamā robežās. Vispārēja piekļuve visiem saglabātajiem datiem, kas nav atkarīga no jebkādas, kaut arī netiešas, saiknes ar sasniedzamo mērķi, nevar tikt uzskatīta par tādu, kas ir absolūti nepieciešama.[475] Tā kā informācijas par datu plūsmu un atrašanās vietas datu nodošana notiek visaptveroši un nediferencēti, tā vispārīgi attiecas uz visām personām, kas izmanto elektronisko komunikāciju pakalpojumus. Tādējādi valsts iestādes saglabā un nodod datus pat par tām personām, par kurām nav nekādu norāžu, kas ļautu uzskatīt, ka to rīcība varētu apdraudēt (pat netieši vai attāli) valsts drošības intereses, un it īpaši netiek pierādīta saikne starp datiem, kuru nodošana ir paredzēta, un draudiem valsts drošībai.[476] EST atzina, ka tāds valsts tiesiskais regulējums, saskaņā ar kuru valsts iestādei valsts drošības aizsardzības nolūkā ir atļauts elektronisko komunikāciju pakalpojumu sniedzējiem noteikt pienākumu veikt visaptverošu un nediferencētu informācijas par datu plūsmu un atrašanās vietas datu nodošanu drošības dienestiem un izlūkdienestiem, pārsniedz absolūti nepieciešamā robežas un ir pretrunā Hartas 7., 8. un 11. pantam.[477]

EST spriedumā lietā "La Quadrature du Net u. c." vispirms līdzīgi atzina, ka tādi tiesību akti, ar kuriem preventīvi paredzēta informācijas par datu plūsmu, kā arī atrašanās vietas datu visaptveroša un nediferencēta saglabāšana valsts un sabiedrības drošības un aizsardzības mērķu vārdā, nav pretrunā ar ES tiesībām. Situācijās, ja pastāv nopietni draudi valsts drošībai, "kuri izrādās patiesi un faktiski vai paredzami", ir pieļaujama visaptveroša un nediferencēta informācijas par datu plūsmu, kā arī atrašanās vietas datu saglabāšana un nodošana. Tādējādi EST atzina, ka izņēmuma gadījumā ir pieļaujama masveida datu – tālruņu un interneta lietotāju personas datu – saglabāšana un nodošana drošības dienestiem arī preventīvos nolūkos, ja pastāv nopietni draudi valsts drošībai. Tāpat EST norādīja, ka saglabāšanai vajadzētu būt ierobežotai laikā, un tas ir absolūti nepieciešams, kā arī ir jāievieš efektīvas garantijas un neatkarīgs pārskatīšanas mehānisms.[478]

EST arī norādīja – lai aizsargātu valsts drošību, apkarotu smagus noziegumus un novērstu nopietnus draudus sabiedrības drošībai, var tikt veikta informācijas par datu plūsmu un atrašanās vietas datu mērķorientēta saglabāšana, kura, pamatojoties uz objektīviem un nediskriminējošiem elementiem, tiek ierobežota atkarībā no attiecīgo personu kategorijām vai pamatojoties uz ģeogrāfisku kritēriju uz laiku, kas nepārsniedz absolūti nepieciešamo, kuru tomēr var pagarināt.

474 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 73. punkts.

475 Turpat, 78. punkts.

476 Turpat, 80. punkts.

477 Turpat, 81. punkts.

478 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 177., 192. punkts.

Tāpat, lai sasniegtu minētos mērķus, ir atļauta arī visaptveroša un nediferencēta elektronisko sakaru līdzekļu lietotāju identitātes datu un savienojuma avotam piešķirtās IP adreses saglabāšana uz laiku, kas nepārsniedz absolūti nepieciešamo.

EST arī atzina, ka ir pieļaujama datu vākšana un analīze reāllaikā. Proti, elektronisko sakaru pakalpojumu sniedzējiem var noteikt pienākumu automatizēti reāllaikā analizēt un vākt informāciju par datu plūsmu un atrašanās vietas datiem, kā arī par tehniskajiem datiem, kas savākti par gala iekārtu izmantošanu. Šādu automatizētu analīzi var izmantot tikai situācijās, kad valsts saskaras ar nopietniem draudiem valsts drošībai, kas izrādās patiesi un faktiski vai paredzami. Savukārt informāciju par datu plūsmu un atrašanās vietas datus reāllaikā var vākt tikai tad, ja tā attiecas uz personām, attiecībā uz kurām ir pamatots iemesls aizdomām, ka tās kaut kādā veidā ir iesaistītas terorisma darbībās.[479]

EST ar spriedumu "La Quadrature du Net u. c." lietā būtībā akceptē visaptverošu un nediferencētu datu saglabāšanu, lai gan tikai izņēmuma gadījumos un tikai tad, ja tas ir stingri nepieciešams demokrātiskā sabiedrībā un samērīgs ar paredzamo nolūku, turklāt tiek pieprasīts ieviest stingras aizsardzības garantijas. Tādējādi EST pietuvinās ECT pieejai, kas līdzīgi atzīst masveida datu saglabāšanu par pieļaujamu, ja vien tiek ievēroti ierobežošanas kritēriji un aizsardzības garantijas.

Apskatītais EST spriedums krasi kontrastē ar spriedumu lietā C-311/18 "Schrems II", kas tika pieņemts dažus mēnešus iepriekš. EST ar minēto spiedumu otro reizi atzina par spēkā neesošu ES un ASV datu nodošanas līgumu, ņemot vērā ASV pastāvošo novērošanas režīmu. Proti, EST gan 2015. gada spriedumā "Schrems I" lietā, gan 2020. gada jūlija spriedumā "Schrems II" lietā konstatēja, ka Eiropas Komisijas lēmumi par aizsardzības līmeņa pietiekamību datu nodošanai uz ASV, kas veidoja pamatu datu nodošanai no ES uz ASV, ir spēkā neesoši. EST ES un ASV privātuma vairoga atzīšana par spēkā neesošu bija balstīta uz vairākiem faktoriem. Tie ir šādi:

1) ASV tiesībaizsardzības prasību prioritāte pār privātuma vairoga prasībām;[480]
2) nepieciešamo varas pilnvaru ierobežojumu un garantiju trūkums saskaņā ar ASV tiesību aktiem, it īpaši, ņemot vērā proporcionalitātes prasības;[481]
3) efektīvs tiesību aizsardzības līdzekļu trūkums ASV ES datu subjektiem[482] un
4) trūkumi privātuma vairoga ombuda mehānismā.[483]

479 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 192. punkts.

480 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 164. punkts.

481 Turpat, 168.–185. punkts.

482 Turpat, 191.–192. punkts.

483 Turpat, 193.–197. punkts. Sk. vairāk Kuner, C. (17 July, 2020). The Schrems II judgment of the Court of Justice and the future of data transfer regulation. *European Law Blog.* https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

EST noraidīja Eiropas Komisijas skaidrojumu, ka ASV valsts iestāžu iejaukšanās to personu pamattiesībās, kuru dati privātuma vairoga ietvaros no ES tiek nosūtīti uz ASV, ja tas notiek valsts drošības, tiesībaizsardzības vai citu valsts interešu nolūkos, un sekojošie ierobežojumi, kas noteikti pašsertificētām organizācijām attiecībā uz to principialitāti, būs ierobežoti līdz tādam apmēram, kas ir absolūti nepieciešams, lai sasniegtu attiecīgo likumīgo mērķi, un tādējādi tie nodrošina efektīvu tiesisko aizsardzību pret šādu iejaukšanos. EST gluži pretēji secināja, ka tiesību normas, uz kurām ir balstīta novērošanas programma, neatbilst minimālajām prasībām, kas ES tiesībās izriet no samērīguma principa, un nevar uzskatīt, ka tās ir ierobežotas līdz absolūti nepieciešamajam.[484] EST secināja, ka privātuma vairogs nenodrošina aizsardzību, kas ir līdzvērtīga Hartā noteiktajām pamattiesībām, jo datiem, kas pārsūtīti saskaņā ar minēto lēmumu, ASV iestādes varēja piekļūt un tos turpmāk apstrādāt, pārsniedzot to, kas ir stingri nepieciešams un samērīgs ar valsts drošības aizsardzības nolūku. "Schrems II" spriedums pieprasa ņemt vērā divas specifiskas prasības: pirmkārt, spriedums nosaka nepieciešamību pēc tiesiskās aizsardzības līdzekļiem, proti, ir jāparedz efektīvas un izpildāmas individuālas pārsūdzības tiesības neatkarīgas un objektīvas tiesas priekšā[485], un, otrkārt, attiecībā uz noteiktu novērošanas programmu apjomu – ir jāparedz ierobežojumi valsts iestāžu piekļuvei personas datiem, lai netiktu pārkāpts absolūtas nepieciešamības un proporcionalitātes princips.[486]

ES un ASV privātuma vairogs nav vienīgais datu nodošanas līgums, ko EST ir atzinusi par spēkā neesošu. 2017. gadā EST pieņēma Atzinumu 1/15 par Nolīguma projektu starp Kanādu un ES par pasažieru datu reģistra datu pārsūtīšanu no ES uz Kanādu. EST paziņoja, ka nolīgumu nevar noslēgt tā pašreizējā formā, jo vairāki tā noteikumi nav savienojami ar tiesībām uz privātumu un datu aizsardzību. Lai gan nolīgumam ir leģitīms mērķis, t. i., sabiedrības drošība un terorisma apkarošana, vairāki tā noteikumi neaprobežojas tikai ar to, kas ir absolūti nepieciešams, un tajā nav paredzēti skaidri un precīzi noteikumi, piemēram, par sensitīvu datu apstrādi. EST atzina, ka visu aviopasažieru datu turpmāka glabāšana pēc pasažieru izlidošanas neaprobežojās tikai ar to, kas ir absolūti nepieciešams, un tā būtu jāattiecina tikai uz tiem pasažieriem, kuru gadījumā ir objektīvas pazīmes, kas liecina, ka viņi varētu radīt risku saistībā ar cīņu pret terorismu un smagiem starptautiskiem noziegumiem. 2020. gada martā Vācijas tiesa uzdeva EST prejudiciālo jautājumu, vai pamattiesībām atbilst Eiropas pasažieru datu saglabāšanas

484 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 167., 184. punkts.

485 Turpat, 167., 184. punkts.

486 Turpat, 179., 180., 183., 185. punkts.

direktīva, kas ļauj iestādēm analizēt un uzglabāt to cilvēku personas datus, kuri veic starptautiskos lidojumus Eiropā.[487]

Gan EST, gan ECT turpina izskatīt lietas par liela apjoma datu saglabāšanu, nodošanu un novērošanu drošības nolūkos. Sagaidāms, ka nākotnē tām būs jāizskata arī lietas par mākslīgā intelekta tehnoloģiju izmantošanas atbilstību cilvēktiesībām. Tajā pašā laikā jau šobrīd judikatūrā izstrādātās būtiskās garantijas ir attiecināmas arī uz jauniem masveida datu vākšanas un novērošanas pasākumiem, to skaitā tādiem, kas izmanto mākslīgā intelekta tehnoloģijas.

5.3. Būtiskās garantijas novērošanas pasākumiem

No abu Eiropas pārnacionālo tiesu judikatūras ir identificējamas vairākas būtiskas garantijas, kas jāievēro, lai nodrošinātu, ka tiesību uz privātumu un datu aizsardzību ierobežošana, piemērojot novērošanas pasākumus, ir proporcionāla un nepieciešama demokrātiskā sabiedrībā.

EST praksē ir plaši vērtēts, vai indivīdu tiesību ierobežojumi atbilst 52. panta nosacījumiem un it īpaši – vai tie ir noteikti tiesību aktos un vai ir samērīgi un nepieciešami demokrātiskā sabiedrībā. EST uzsver arī neatkarīgas iestādes kontroles nozīmi, kas paredzēta Hartas 8. panta 3. punktā, kā arī efektīvu tiesību aizsardzības līdzekļu nozīmi, kas ir noteikti Hartas 47. pantā. Līdzīgi arī ECT praksē ir atzīts, ka indivīdu tiesību ierobežojumam ir jābūt noteiktam ar likumu, tam ir jābūt samērīgam un nepieciešamam demokrātiskā sabiedrībā, kā arī ir jābūt efektīviem tiesību aizsardzības līdzekļiem, ko var izmantot aizskartās personas. Eiropas Datu aizsardzības kolēģija 2020. gada novembrī publicēja Ieteikumus 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem, kura tika izstrādāta pēc EST "Schrems II" sprieduma pieņemšanas. Tā tika sagatavota, balstoties uz iepriekš 2016. gadā 29. panta darba grupas izstrādāto dokumentu 01/2016 par pamatojumu pamattiesību uz privātumu un datu aizsardzību ierobežošanai, izmantojot novērošanas pasākumus personas datu nosūtīšanas gadījumā[488], un kurš savukārt tika publicēts pēc EST "Schrems I" sprieduma. Abos dokuments ir norādīts, ka tiesiskās prasības, kuras izriet no EST un ECT judikatūras masveida novērošanas lietās un kuras ir jāievēro, lai privātuma un datu

487 Lūgums sniegt prejudiciālu nolēmumu, ko 2020. gada 27. maijā iesniedza *Verwaltungsgericht Wiesbaden* (Vācija) – OC/*Bundesrepublik Deutschland*, EST lieta C-148/20, ES OV, C 279/30, 24.08.2020.

488 Article 29 Data Protection Working Party. (2016). Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees). https://ec.europa.eu/newsroom/article29/items/640363/en

aizsardzības ierobežojumi varētu tikt uzskatīti par attaisnojamiem saskaņā ar Hartu, var apkopot četrās būtiskās garantijās:

1) apstrādei jābalstās uz skaidru, precīzu un pieejamu regulējumu;
2) ir jāpierāda nepieciešamība un samērīgums attiecībā uz izvirzītajiem likumīgajiem mērķiem;
3) jāpastāv neatkarīgam uzraudzības mehānismam;
4) personām ir jābūt pieejamiem efektīviem tiesību aizsardzības līdzekļiem.[489]

Nodaļas turpinājumā konkrētāk aplūkots, ko paredz katra no šīm būtiskajām garantijām.

5.3.1. Skaidrs, precīzs un pieejams regulējums

Pirmais nosacījums, kas ir jāpārbauda, kad ir konstatēts, ka pastāv iejaukšanās tiesībās uz datu aizsardzību, ir – vai šāda iejaukšanās ir "paredzēta likumā".

Minētā prasība ir ietverta Hartas 52. panta 1. punktā, kas nosaka, ka visiem Hartā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jābūt paredzētiem tiesību aktos. Turklāt Hartas 8. panta 2. punkts paredz personas datu apstrādes nosacījumus, proti, ka šādi dati ir jāapstrādā godprātīgi, noteiktiem mērķiem un ar likumīgu pamatojumu, kas paredzēts tiesību aktos.

Hartā noteiktā prasība, saskaņā ar kuru jebkuram pamattiesību ierobežojumam ir jābūt noteiktam tiesību aktos, nozīmē, ka pašā juridiskajā pamatā ir jānosaka attiecīgo tiesību īstenošanas ierobežojuma apjoms. Juridiskajā pamatā, kas ļauj iejaukties pamattiesībās, lai tas atbilstu samērīguma principam, ir arī jāparedz skaidri un precīzi noteikumi attiecībā uz konkrētā pasākuma tvērumu un piemērošanu, kā arī minimālās aizsardzības garantijas.[490] EST turklāt atgādina, ka personām garantētajām tiesībām ir jābūt efektīvām un īstenojamām.

EST "Schrems II" lietā konstatēja, ka no attiecīgā ASV tiesiskā regulējuma neizriet ne tas, ka pastāv pilnvaru ierobežojumi novērošanas programmu īstenošanai ārējās izlūkošanas mērķiem, ne arī garantijas personām, kuras nav ASV pilsoņi un kuras potenciāli skar šīs programmas, tādējādi nevar tikt nodrošināts tāds aizsardzības līmenis, kas būtībā būtu līdzvērtīgs Hartā garantētajam. Tāpat tā konstatēja, ka datu subjektiem, kuru dati ir pārsūtīti uz attiecīgo trešo valsti, nav piešķirtas tiesības, kuras viņi tiesās varētu īstenot pret ASV iestādēm. Līdz ar to privātuma vairogs, pretēji tam, kas noteikts VDAR 45. panta 2. punkta

489 Eiropas Datu aizsardzības kolēģija. (2020). Ieteikumi 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_lv

490 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 175., 180., 181. punkts; EST 2017. gada 26. jūlija atzinums 1/15 *Accord PNR UE-Canada*, ECLI:EU:C:2017:592, 139. punkts un tajā minētā judikatūra.

a) apakšpunktā, nevar nodrošināt būtībā līdzvērtīgu aizsardzības līmeni tam, kāds izriet no Hartas.[491]

EST lietā "Privacy International" līdzīgi norādīja – lai izpildītu samērīguma prasību, tiesiskajā regulējumā ir jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma tvērumu un piemērošanu un paredz minimālās prasības, lai tā rezultātā personām, kuru personas dati tikuši pārsūtīti, būtu pietiekamas garantijas, kas ļautu šos datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku. Šim tiesiskajam regulējumam ir jābūt juridiski saistošam valsts tiesībās, un tajā it īpaši ir jānorāda, kādos apstākļos un ar kādiem nosacījumiem var īstenot pasākumu, kas ietver šādu datu apstrādi, tādējādi garantējot, ka šāda iejaukšanās notiek tikai absolūti nepieciešamās robežās. Šādu garantiju sniegšanas nepieciešamība ir vēl jo svarīgāka tādēļ, ka personas dati tiek apstrādāti automātiski un pastāv ievērojams nelikumīgas piekļuves risks šiem datiem. Šie apsvērumi ir it īpaši svarīgi, ja runa ir par tādas kategorijas personas datu aizsardzību kā sensitīvi dati.[492]

ECT ir vērsusi uzmanību – nosacījums, ka pamattiesību ierobežošanai ir jābūt "paredzētai likumā", nozīmē: novērošanas pasākumam ir jābūt zināmam pamatam nacionālajā likumdošanā un tam jāatbilst tiesiskuma principam.[493] ECT judikatūrā ir noteiktas sešas minimālās aizsardzības garantijas, kas ir jāparedz tiesiskajā regulējumā attiecībā uz slepenu novērošanas pasākumu piemērošanu, lai izvairītos no varas ļaunprātīgas izmantošanas:

1) nodarījumu jeb pārkāpumu veids, kas var izraisīt noklausīšanās rīkojumu;
2) to cilvēku kategorijas, kuru tālruņus var noklausīties;
3) telefona sarunu noklausīšanās ilguma ierobežojums;
4) kārtība, kas jāievēro, pārbaudot, izmantojot un uzglabājot iegūtos datus;
5) piesardzības pasākumi, kas jāievēro, paziņojot datus citām pusēm;
6) apstākļi, kādos ierakstus var vai ir nepieciešams izdzēst vai iznīcināt.[494]

491 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 180., 181. punkts.

492 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 68. punkts un tajā minētā judikatūra. Sk. arī EST 2014. gada 8. aprīļa spriedumu apvienotajās lietās C293/12 .., 55. punkts; EST 2016. gada 21. februāra spriedumu apvienotajās lietās C-203/15 .., 117. punkts; EST 2017. gada 26. jūlija atzinums 1/15, 141. punkts.

493 European Court of Human Rights (2020), Guide on Article 8 of the Convention, p. 124.

494 ECT 2016. gada 12. janvāra spriedums lietā 37138/14, 56. punkts; ECT 2015. gada 4. decembra spriedums lietā 47143/06, 231., 238.–301. punkts; ECT 2000. gada 16. februāra spriedums lietā 27798/95 *Amann v. Switzerland*, 56.–58. punkts.

Likumā ir jānorāda arī izpildvarai vai tiesnesim piešķirtās rīcības brīvības apjoms un tā izmantošanas veids ar pietiekamu skaidrību, lai indivīdam nodrošinātu pietiekamu aizsardzību pret patvaļīgu iejaukšanos.[495]

Viens no galvenajiem nosacījumiem, ko ir uzsvērusi ECT, – likumam jābūt pieejamam attiecīgajai personai un paredzamam attiecībā uz tā sekām.[496] Sakaru pārtveršanas kontekstā "paredzamību" nevar saprast tāpat kā daudzās citās jomās. Paredzamība slepenu novērošanas pasākumu kontekstā nenozīmē, ka indivīdiem jāspēj paredzēt, kad iestādes, iespējams, pārtver viņu saziņu, lai viņi varētu attiecīgi pielāgot savu rīcību.[497] Tomēr, lai izvairītos no patvaļīgas iejaukšanās, ir svarīgi, lai būtu skaidri, detalizēti noteikumi par tālruņa sarunu pārtveršanu. Likumam jābūt pietiekami skaidram, lai iedzīvotājiem sniegtu atbilstošu norādi par apstākļiem un nosacījumiem, kādos valsts iestādes ir pilnvarotas izmantot šādus slepenus pasākumus.[498]

Šajā ziņā pasākumiem jābūt paredzamiem un pieejamiem personām, kuras arī ir jāinformē par valsts iestāžu iespējamo piekļuvi datiem, ko šīs personas sniedz privātiem uzņēmumiem, lai saņemtu pakalpojumu, piemēram, rezervējot lidojumu, pārskaitot naudu, nosūtot e-pastu vai īsziņu vai pārlūkojot internetu. Novērošanas programmas, kas gadiem ilgi darbojas slepeni un ko atklāja plašsaziņas līdzekļi vai trauksmes cēlēji, piemēram, PRISM, neatbilst šīm prasībām.[499]

Nosacījums, ka ierobežojumiem ir jābūt skaidri un precīzi noteiktiem tiesiskajā regulējumā, ir attiecināms arī uz valsts iestāžu novērošanas pasākumiem, kas balstās uz jaunajām tehnoloģijām, tostarp sejas atpazīšanas tehnoloģijām. Šādus pasākumus nevar īstenot slepeni, tos skaidri nenosakot tiesību aktos. Tiesiskajā regulējumā ir jāparedz, kādi ir to piemērošanas apstākļi un nosacījumi, kādas personas tas skar, kādas aizsardzības garantijas tiek piemērotas, kā arī kādas ir personu iespējas efektīvi aizsargāt savas tiesības. Prasības pēc atbilstoša tiesiskā regulējuma izriet arī no datu aizsardzības prasībām (tas atklāts grāmatas

495 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 230. punkts; ECT 1984. gada 2. augusta spriedums lietā 8691/79, 68. punkts; ECT 1990. gada 24. aprīļa spriedums lietā 11105/84 *Huvig v. France,* 29. punkts; ECT 2006. gada 29. jūnija lēmums lietā 54934/00 *Weber and Saravia v. Germany*, 94. punkts.

496 ECT 2010. gada 18. maija spriedums lietā 26839/05 *Kennedy v. the United Kingdom*, 151. punkts; ECT 2015. gada 4. decembra spriedums lietā 47143/06, 229. punkts.

497 ECT 2006. gada 29. jūnija lēmums lietā 54934/00, 93. punkts.

498 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 229. punkts; ECT 2007. gada 28. jūnija spriedums lietā *The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 75. punkts; ECT 2018. gada 13. septembra spriedums .. 58170/13, 62322/14, 24960/15, 307. punkts.

499 Tzanou (2019), *The Fundamental Right to Data Protection*, p. 253.

sestajā nodaļā), tajā pašā laikā tās tiešā veidā izriet arī no prasības, ka cilvēktiesību ierobežojumiem ir jābūt noteiktiem tiesību aktā.

Tomēr tas vien, ka ierobežojumi ir noteikti tiesību aktā, vēl nenozīmē, ka tie ir likumīgi. Nākamais nosacījums, kas jāpārbauda, ir samērīgums un nepieciešamība.

5.3.2. Samērīgums un nepieciešamība

Hartas 52. panta 1. punkta pirmais teikums paredz, ka visiem Hartā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jārespektē šo tiesību un brīvību būtība. Tālāk minētās normas otrais teikums paredz, ka, ievērojot proporcionalitātes principu, ierobežojumus drīkst uzlikt tikai tad, ja tie ir nepieciešami un patiešām atbilst vispārējas nozīmes mērķiem, ko atzinusi ES, vai vajadzībai aizsargāt citu personu tiesības un brīvības.

Satversmes tiesa, izvērtējot pamattiesību ierobežojumu samērīgumu, pārbauda trīs aspektus:

1) vai izraudzītie līdzekļi ir piemēroti leģitīmā mērķa sasniegšanai, proti, vai ar izraudzīto līdzekli var sasniegt leģitīmo mērķi;
2) vai šāda rīcība ir nepieciešama, proti, vai leģitīmo mērķi nevar sasniegt ar indivīda tiesības mazāk ierobežojošiem līdzekļiem;
3) vai ierobežojums ir atbilstošs, proti, vai labums, ko iegūst sabiedrība, ir lielāks par indivīda tiesībām nodarīto kaitējumu.

Ja tiek atzīts, ka pamattiesību ierobežojums neatbilst kaut vienam no šiem kritērijiem, tad tas neatbilst samērīguma principam un ir prettiesisks.[500] Attiecībā uz pirmo nosacījumu – likumdevēja izraudzītie līdzekļi ir piemēroti leģitīmā mērķa sasniegšanai, ja ar konkrēto regulējumu šis mērķis tiek sasniegts.[501] Attiecībā uz otro nosacījumu – pamattiesību ierobežojums ir nepieciešams, ja nepastāv citi līdzekļi, kuri būtu tikpat iedarbīgi un kurus izvēloties personu pamattiesības tiktu ierobežotas mazāk.[502]

EST izmanto līdzīgu pieeju, lai izvērtētu samērīguma principa ievērošanu. Turklāt saskaņā ar tās pastāvīgo judikatūru atkāpes un ierobežojumi personas datu aizsardzībai ir jāpiemēro tikai tiktāl, ciktāl tas ir "absolūti nepieciešams".

EST spriedumā apvienotajās lietās "Digital rights Ireland" un "Seitlinger u. c." norāda, ka atbilstoši samērīguma principam ES iestāžu tiesību aktiem ir jābūt piemērotiem attiecīgajā tiesiskajā regulējumā noteikto leģitīmo mērķu sasniegšanai

500 Sk., piemēram, Satversmes tiesas 2020. gada 18. novembra spriedums lietā Nr. 2019-32-01, 16. punkts.

501 Turpat, 17. punkts.

502 Turpat, 18. punkts.

un tie nedrīkst pārsniegt to, kas ir to sasniegšanai atbilstošs un nepieciešams.[503] ES likumdevēja novērtējuma brīvība var būt ierobežota atkarībā no daudziem faktoriem, tostarp no skartās jomas, attiecīgo Hartā garantēto tiesību rakstura, iejaukšanās rakstura un būtiskuma, kā arī tās mērķa.[504] Tajā pašā laikā tiesību uz privātās dzīves neaizskaramību aizsardzība katrā ziņā prasa, lai atkāpes no personas datu aizsardzības un tās ierobežojumi tiktu īstenoti "absolūti nepieciešamā" ietvaros.[505] Minētajā lietā EST atzina, ka Datu saglabāšanas direktīva ES tiesību sistēmā rada plaša apjoma un īpaši būtisku iejaukšanos Hartas 7. un 8. pantā garantētajās pamattiesībās un šī iejaukšanās nav precīzi reglamentēta ar tiesību normām, kas ļautu nodrošināt, lai tā patiešām būtu ierobežota ar "absolūti nepieciešamo".

Arī attiecībā uz ES dalībvalstu tiesību aktiem EST lietā "Privacy International" atzina, ka valsts tiesiskais regulējums, kas valsts iestādei valsts drošības aizsardzības nolūkā atļauj elektronisko komunikāciju pakalpojumu sniedzējiem noteikt pienākumu veikt visaptverošu un nediferencētu informācijas par datu plūsmu un atrašanās vietas datu nodošanu drošības dienestiem un izlūkdienestiem, pārsniedz absolūti nepieciešamā robežas.[506]

EST ir norādījusi, ka dalībvalstu piemērotie tiesību ierobežojumi ir jāizvērtē, izsverot iejaukšanās, ko rada šāds ierobežojums, smagumu, un pārbaudot, vai vispārējo interešu mērķa nozīmīgums, kas ir šī ierobežojuma pamats, ir atbilstošs šim smagumam.[507]

EST spriedumā lietā "La Quadrature du Net u. c.", atsaucoties uz tās pastāvīgo judikatūru, atkārtoti uzsver, ka pamattiesību uz privātās dzīves neaizskaramību aizsardzība atbilstoši tās pastāvīgajai judikatūrai nozīmē, ka atkāpes no personas datu aizsardzības un tās ierobežojumi ir jāīsteno, ja tas ir "absolūti nepieciešams". Turklāt vispārējo interešu mērķi nevar sasniegt, neņemot vērā to, ka tas ir jāsaskaņo ar pamattiesībām, uz kurām attiecas pasākums, līdzsvarojot vispārējo interešu mērķi, no vienas puses, ar attiecīgajām tiesībām, no otras puses.[508]

Izvērtējot valstu masveida novērošanas pasākumu likumību, EST un ECT judikatūrā pamatā tiek samērotas personas tiesības uz privātumu un datu aizsardzību, no vienas puses, ar valsts drošības, sabiedrības drošības un noziedzības apkarošanas interesēm, no otras puses. EST lietā "La Quadrature du Net u. c.", kas

503 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C293/12 .., 46. punkts.

504 Turpat, 47. punkts.

505 Turpat, 52. punkts.

506 EST 2020. gada 6. oktobra spriedums lietā C-623/17, 81. punkts.

507 Turpat, 131. punkts.

508 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 130. punkts; EST 2020. gada 6. oktobra spriedums lietā C-623/17, 68. punkts

saistīta ar dalībvalsts tiesību aktiem, nolēma, ka valsts drošības aizsardzības mērķis tā svarīguma dēļ spēj attaisnot pasākumus, kas rada būtiskāku pamattiesību aizskārumu, bet ne pasākumus, kurus varētu pamatot ar citiem mērķiem, piemēram, noziedzības apkarošanu. Tomēr tā konstatēja, ka tas tā ir, ja ir pietiekami nopietni iemesli uzskatīt, ka attiecīgā valsts saskaras ar nopietniem draudiem valsts drošībai, kas ir pierādīti kā patiesi un faktiski vai paredzami un ir pakļauti citu Hartas 52. panta 1. punktā noteikto prasību izpildei.[509]

Jautājums, vai ierobežojumi ir samērīgi un nepieciešami, ir izvērtējams kopsakarā ar pirmo, iepriekš aplūkoto nosacījumu, t. i., kādā veidā ierobežojumi ir paredzēti tiesību aktā. EST "Schrems II" lietā norāda – lai izpildītu samērīguma prasību, attiecīgajā tiesiskajā regulējumā, kas paredz datu aizsardzības ierobežojumus, ir jānosaka skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma tvērumu un piemērošanu un paredz minimālas prasības, lai tā rezultātā personām, kuru dati tikuši pārsūtīti, būtu pietiekamas garantijas, kas ļautu viņu personas datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku. Tajā it īpaši ir jānorāda, kādos apstākļos un saskaņā ar kādiem nosacījumiem šādu datu apstrādi paredzošs pasākums var tikt veikts, tādējādi garantējot, ka šāda iejaukšanās notiek tikai stingri nepieciešamajā apmērā.[510]

Arī saskaņā ar ECT praksi prasība, ka ierobežojumam ir jābūt "paredzētam likumā", ir jāvērtē kopsakarā ar nepieciešamības un samērīguma prasību. ECTK 8. panta 2. punkts paredz: "Sabiedriskās institūcijas nedrīkst traucēt nevienam baudīt šīs tiesības [uz privātās dzīves neaizskaramību], izņemot gadījumos, kas ir paredzēti likumā un nepieciešami demokrātiskā sabiedrībā, lai aizsargātu valsts drošības, sabiedriskās kārtības vai valsts labklājības intereses, lai nepieļautu nekārtības vai noziegumus, lai aizsargātu veselību vai morāli, vai lai aizstāvētu citu tiesības un brīvības." ECT ir atzinusi, ka "tiesību kvalitāte" nozīmē, ka nacionālajiem tiesību aktiem jābūt ne tikai pieejamiem un paredzamiem attiecībā uz to piemērošanu, bet arī jānodrošina, lai slepeni novērošanas pasākumi tiktu piemēroti tikai tad, kad tas ir "nepieciešams demokrātiskā sabiedrībā", it īpaši jāparedz adekvātas un efektīvas aizsardzības garantijas pret ļaunprātīgu izmantošanu.[511] Valsts iestādēm ir zināma rīcības brīvība. Tomēr šī brīvība ir pakļauta Eiropas tiesību uzraudzībai, kas ietver gan tiesību aktus, gan lēmumus to piemērošanā. Tiesai jābūt pārliecinātai, ka pastāv pietiekamas un efektīvas garantijas pret ļaunprātīgu izmantošanu.[512] Šī jautājuma novērtējums ir atkarīgs no visiem lietā apskatāmajiem apstākļiem, piemēram, no iespējamo pasākumu rakstura,

509 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 168. punkts.

510 EST 2020. gada 16. jūlija spriedums lietā C-311/18, 176. punkts.

511 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 236. punkts.

512 ECT 1978. gada 6. septembra spriedums lietā 5029/71, 50. punkts.

apjoma un ilguma, iemesliem, kas nepieciešami, lai tos piemērotu, no iestādēm, kas ir kompetentas tos atļaut, veikt un uzraudzīt, kā arī no tiesību aizsardzības līdzekļu veida. Ierobežojošo pasākumu noteikšanas un ieviešanas uzraudzības procedūrām jābūt tādām, lai saglabātu "iejaukšanos" tādu, kas ir "nepieciešama demokrātiskā sabiedrībā".[513]

Līdzīgi kā EST, arī ECT ir norādījusi, ka valsts slepeniem novērošanas pasākumiem ir jāatbilst "stingras nepieciešamības" kritērijam. Jebkādu iejaukšanos tiesībās uz privātumu atbilstoši ECTK 8. panta 2. punktam var attaisnot tikai tad, ja tā ir saskaņā ar likumu, tai ir viens vai vairāki likumīgi mērķi, kas noteikti minētajā normā, un tā ir nepieciešama demokrātiskā sabiedrībā, lai sasniegtu šādu mērķi. Tā kā šis noteikums paredz izņēmumu no tiesībām, kuras garantē ECTK, tas ir jāinterpretē šauri. Lietā "Klāss un citi pret Vāciju" ECT nosprieda, ka "pilsoņu slepenas novērošanas pilnvaras saskaņā ar ECTK ir pieļaujamas tikai tiktāl, ciktāl tas ir nepieciešams demokrātisku institūciju aizsardzībai"[514].

ECT lietā "Szabó un Vissy pret Ungāriju" arī atzīst, ka izteiciens "absolūti nepieciešams" no pirmā acu uzmetiena ir tests, kas atšķiras no tā, kas noteikts ECTK 8. panta 2. punkta redakcijā, tas ir, "nepieciešams demokrātiskā sabiedrībā".[515] Ņemot vērā attiecīgās iejaukšanās īpašo raksturu un modernāko novērošanas tehnoloģiju potenciālo aizskārumu pilsoņu privātumam, ECT uzskata, ka prasība "nepieciešams demokrātiskā sabiedrībā" ir jāinterpretē kā prasība pēc "stingras nepieciešamības" divos aspektos. Var uzskatīt, ka slepeni novērošanas pasākumi atbilst ECTK tikai tad, ja tas ir absolūti nepieciešams demokrātisku institūciju aizsardzībai, un turklāt, ja tas ir absolūti nepieciešams vitāli svarīgas informācijas iegūšanai individuālā operācijā. Jebkurš slepens novērošanas pasākums, kas neatbilst "stingras nepieciešamības" kritērijam, var būt pakļauts varas iestāžu ļaunprātīgai izmantošanai ar to rīcībā esošajām tehnoloģijām. Turklāt ECT vērš uzmanību, ka gan EST, gan ANO īpašais referents jautājumos par uzskatu un vārda brīvības tiesību veicināšanu un aizsardzību pieprasa, lai slepeni novērošanas pasākumi atbilstu stingras nepieciešamības kritērijam. Turklāt šajā kontekstā ECT īpaši uzsver iepriekšējas tiesas atļaujas nozīmi. Šī garantija ļauj ierobežot tiesībaizsardzības iestāžu rīcības brīvību, interpretējot plašu jēdzienu – "attiecīgās personas, kas identificētas [..] kā personu loks", lai pārbaudītu, vai katrā konkrētajā gadījumā personas saziņas pārtveršanai ir pietiekami iemesli. Tikai

513 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 232. punkts un tajā citētā judikatūra.

514 ECT 1978. gada 6. septembra spriedums lietā 5029/71, 42. un 54. punkts. Skat. arī ECT 2016. gada 12. janvāra spriedumu lietā 37138/14, 54. punkts.

515 ECT 2016. gada 12. janvāra spriedums lietā 37138/14, 72. punkts.

tādā veidā var apmierināt nepieciešamību pēc drošības pasākumiem, lai ārkārtas pasākumus izmantotu ierobežoti un tikai pienācīgi pamatotos gadījumos.[516]

Norāde, ka iejaukšanās "nepieciešama demokrātiskā sabiedrībā", ir jāinterpretē kā prasība, lai visi veiktie pasākumi būtu "absolūti nepieciešami" gan kā vispārējs apsvērums, lai aizsargātu demokrātiskas institūcijas, gan kā īpašs apsvērums, lai iegūtu būtisku informāciju konkrētajā gadījumā, lai novērstu draudus valsts vai sabiedrības drošībai vai noziedzīgu nodarījumu atklāšanai un nepieļaušanai.

ECT norādītie apsvērumi ir būtiski, izvērtējot jaunu mākslīgā intelekta novērošanas tehnoloģiju ieviešanu un izmantošanu. Pirms šādu tehnoloģiju ieviešanas ir jāizvērtē, vai tās ir vajadzīgas, jo "var palīdzēt" un "ir piemērotas", lai sasniegtu konkrēto mērķi, piemēram, lai garantētu valsts drošību, vai arī tās ir "stingri nepieciešamas" un nepastāv citu mazāk tiesības ierobežojošu veidu un līdzekļu, kā šo mērķi sasniegt. Tikai pēdējā gadījumā ierobežojumi var tikt atzīti par tiesiskiem.

5.3.3. Neatkarīgs uzraudzības mehānisms

Jau kopš 1978. gada lietas "Klāss un citi pret Vāciju" ECT daudzas reizes ir nospriedusi, ka ir būtiski, lai jebkāda iejaukšanās tiesībās uz privātumu un datu aizsardzību būtu pakļauta efektīvai, neatkarīgai un objektīvai uzraudzības sistēmai, ko nodrošina vai nu tiesnesis, vai cita neatkarīga struktūra. ECT ir norādījusi, ka slepenu novērošanas pasākumu pārbaude un uzraudzība var notikt trīs posmos: kad novērošana tiek noteikta pirmo reizi, kamēr tā tiek veikta un pēc tās izbeigšanas. Attiecībā uz pirmajiem diviem posmiem slepenas novērošanas būtība un loģika nosaka, ka tā jāveic bez personas ziņas. Līdz ar to, tā kā indivīdam obligāti tiks liegts pašam izmatot efektīvus tiesiskās aizsardzības līdzekļus vai tieši piedalīties jebkādās pārskatīšanas procedūrās, ir svarīgi, lai noteiktais process sniegtu pietiekamas un līdzvērtīgas garantijas, kas aizsargā viņa tiesības. Turklāt novērošanas procesā pēc iespējas precīzāk jāievēro demokrātiskas sabiedrības vērtības, lai netiktu pārsniegtas nepieciešamības robežas ECTK 8. panta 2. punkta izpratnē.

ECT ir norādījusi, ka slepenās novērošanas jomā, kur ļaunprātīga izmantošana ir potenciāli vienkārša un varētu radīt kaitīgas sekas demokrātiskai sabiedrībai kopumā, principā ir vēlams novērošanas kontroli uzticēt tiesnesim, ņemot

516 ECT 2016. gada 12. janvāra spriedums lietā 37138/14, 73. punkts.

vērā, ka tiesas kontrole nodrošina labākās neatkarības, objektivitātes un taisnīguma garantijas un pareizu procesa veikšanu.[517]

Kas attiecas uz trešo posmu, pēc novērošanas pabeigšanas jautājums par novērošanas pasākumu turpmāku paziņošanu ir nesaraujami saistīts ar tiesvedībā izmantojamo tiesiskās aizsardzības līdzekļu efektivitāti un līdz ar to ar efektīvu garantiju esamību pret novērošanas pilnvaru ļaunprātīgu izmantošanu. Attiecīgajai personai principā ir maz iespēju vērsties tiesā, izņemot, ja pastāv šādi apstākļi: ja persona ir informēta par pasākumu veikšanu bez viņa ziņas, un tādējādi tā ar atpakaļejošu spēku var apstrīdēt pasākumu likumību; vai arī – tiesā var vērsties jebkura persona, kurai ir aizdomas, ka tās saziņa tiek vai ir pārtverta, bet tiesas piekritība nedrīkstētu būt atkarīga no tā, vai šai personai ir paziņots, ka tās saziņa tikusi pārtverta.[518]

Tajā pašā laikā ECT 2018. gada spriedumā apvienotajās lietās "Big Brother Watch u. c. pret Apvienoto Karalisti" vērš uzmanību, ka objektīvu pierādījumu pieprasīšana par pamatotām aizdomām attiecībā uz personām, par kurām tiek meklēti dati, un sekojošais paziņojums novērošanas subjektam būtu pretrunā ar ECT atziņu, ka liela apjoma datu pārtveršanas režīma darbība principā ietilpst valsts rīcības brīvībā. Liela apjoma datu pārtveršana pēc definīcijas nav mērķtiecīga, un, pieprasot "pamatotas aizdomas", šādas shēmas darbība būtu neiespējama. Tāpat prasība par "turpmāku paziņošanu" paredz skaidri definētu novērošanas mērķu esamību, kas vienkārši nenotiek lielapjoma pārtveršanas režīmā. Turpretim tiesas atļauja pēc būtības nav nesaderīga ar masveida pārtveršanas efektīvu darbību.[519]

ECT lietā vērš uzmanību, ka tā jau iepriekš ir norādījusi – "vēlams novērošanas jurisdikciju uzticēt tiesnesim", jo novērošanas slepenā rakstura dēļ indivīds parasti nevarēs pats izmeklēt tiesiskās aizsardzības līdzekļus. Tajā pašā laikā ECT iepriekš to nav uzskatījusi "nepieciešamu prasību". ECT norāda, ka "negodīga, nolaidīga vai pārāk dedzīga ierēdņa nepareizas rīcības iespēju nekad nevar pilnībā izslēgt neatkarīgi no sistēmas". ECT atsaucas uz tās iepriekšējo judikatūru, kur var atrast daudzus piemērus gadījumiem, kad iepriekšēja tiesas atļauja nodrošināja tikai ierobežotu aizsardzību pret datu ļaunprātīgu izmantošanu vai to vispār nenodrošināja.[520] Piemēram, lietā "Roman Zakharov pret Krieviju" jebkurai saziņas pārtveršanai bija jāsaņem tiesas atļauja, un tiesnesim bija jāpamato

517 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 233. punkts; ECT 1978. gada 6. septembra spriedums lietā 5029/71, 55.–56. punkts.

518 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 234. punkts; ECT 1978. gada 6. septembra spriedums lietā 5029/71, 57. punkts.

519 ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13 .., 310., 315.–320. punkts.

520 Turpat, 319. punkts.

lēmums atļaut datu pārtveršanu. Tomēr, tā kā tiesas pārbaudes darbības joma bija ierobežota un policijai bija tehniski līdzekļi, lai apietu atļaujas piešķiršanas procedūru un pārtvertu jebkādu saziņu, iepriekš nesaņemot tiesas atļauju, ECT atzina, ka Krievijas likumi nespēj nodrošināt, ka "iejaukšanās" nepārkāpj kritērija "nepieciešams demokrātiskā sabiedrībā" robežas.[521] Lietā "Mustafa Sezgin Tanrıkulu pret Turciju" ECT konstatēja ECTK 8. panta pārkāpumu, kad krimināltiesa pusotru mēnesi bija piešķīrusi Nacionālajai izlūkošanas aģentūrai atļauju pārtvert visus vietējos un starptautiskos sakarus, lai identificētu personas, kas tika turētas aizdomās par terorismu.[522]

ECT lietā "Big Brother Watch u. c. pret Apvienoto Karalisti" secina, lai arī tā tiesas atļauju uzskata par svarīgu drošības līdzekli un varbūt pat par labo praksi, pati par sevi tā nevar būt ne vajadzīga, ne pietiekama, lai nodrošinātu ECTK 8. panta ievērošanu. Drīzāk ir jāņem vērā saziņas pārtveršanas sistēmas faktiskā darbība, tostarp varas izmantošanas pārbaudes un līdzsvars, kā arī faktiskas ļaunprātīgas izmantošanas pierādījumu esamība vai neesamība. Attiecīgi ECT izskatīja jebkādas iejaukšanās pamatojumu lietā, atsaucoties uz sešām obligātajām prasībām, kuras iepriekš izstrādātas tās judikatūrā par saziņas pārtveršanu kriminālizmeklēšanā un kuras būtu jānosaka tiesību aktā, lai izvairītos no varas ļaunprātīgas izmantošanas:

1) nodarījumu veids, kas var izraisīt noklausīšanās rīkojumu;
2) to cilvēku kategoriju definīcija, kuru saziņa var tikt pārtverta;
3) pārtveršanas ilguma ierobežojums;
4) prasības, kas jāievēro, pārbaudot, izmantojot un uzglabājot iegūtos datus;
5) piesardzības pasākumi, kas jāievēro, paziņojot datus citām pusēm;
6) apstākļi, kādos pārtvertos datus var dzēst vai iznīcināt.[523]

Lai gan ECT ņēma vērā arī citus attiecīgos faktorus, kurus tā identificēja lietā "Roman Zakharov pret Krieviju", proti, kārtību slepenu novērošanas pasākumu īstenošanas uzraudzībai, jebkuri paziņošanas mehānismi un valsts tiesību aktos paredzētie tiesiskās aizsardzības līdzekļi tomēr nekvalificēja šos pasākumus kā minimālās prasības.

Arī ES regulējums paredz neatkarīgas uzraudzības prasību. Hartas 8. panta 3. punkts nosaka, ka atbilstību tiesībām uz personas datu aizsardzību, kas paredzētas minētā panta 1. un 2. punktā, kontrolē neatkarīga iestāde.

Saistībā ar dalībvalstu tiesību aktiem EST ir identificējusi vairākus pasākumus, kas ir atbilstoši ES tiesību aktiem tikai tad, ja tos efektīvi pārskata tiesa vai administratīva iestāde, kuras lēmums ir saistošs.

521 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 232. punkts.

522 ECT 2017. gada 18. jūnija spriedums lietā 27473/06, 64. punkts.

523 ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13 .., 307., 320. punkts.

EST spriedumā apvienotajās lietās "Tele2 Sverige AB" un "Watson u. c.", atsaucoties uz ECT judikatūru, vērš uzmanību – tā kā vispārēja piekļuve visiem saglabātajiem datiem, kas nav atkarīga no jebkādas, kaut arī netiešas saiknes ar sasniedzamo mērķi, nevar tikt uzskatīta par tādu, kas aprobežojas ar absolūti nepieciešamo, attiecīgajam valsts tiesiskajam regulējumam ir jābalstās uz objektīviem kritērijiem, lai definētu apstākļus un nosacījumus, saskaņā ar kuriem kompetentajām valsts iestādēm piešķir piekļuvi abonentu vai reģistrēto lietotāju datiem. Šajā ziņā piekļuvi saistībā ar mērķi apkarot noziedzību var piešķirt vienīgi to personu datiem, kuras tiek turētas aizdomās par smaga nozieguma plānošanu, sagatavošanos tam vai tā izdarīšanu vai arī kuras vienā vai otrā veidā ir saistītas ar šādu noziegumu. Tomēr īpašos gadījumos, proti, kad vitāli svarīgas valsts drošības, aizsardzības vai sabiedrības drošības intereses apdraud teroristiskas darbības, piekļuvi var piešķirt arī citu personu datiem, ja pastāv objektīvi apstākļi, kas ļauj uzskatīt, ka šie dati konkrētajā gadījumā varētu sniegt efektīvu ieguldījumu šādu darbību apkarošanā.[524] Lai praksē nodrošinātu šo nosacījumu ievērošanu pilnībā, ir būtiski, ka kompetento valsts iestāžu piekļuve saglabātajiem datiem, izņemot atbilstoši pamatotus steidzamības gadījumus, principā ir pakļauta kontrolei un to veic tiesa vai neatkarīga administratīva iestāde, un šīs tiesas vai šīs iestādes lēmums tiek pieņemts pēc tam, kad šīs iestādes iesniegušas pamatotu pieteikumu, tostarp saistībā ar noziedzīga nodarījuma novēršanu, atklāšanu vai kriminālvajāšanas procedūrām.[525]

EST ir vērsusi uzmanību uz neatkarīgas tiesas nozīmi pār novērošanas programmu īstenošanu, kas paredz liela apjoma datu apstrādi, un arī gadījumos, kad tā neattiecas uz individuālu novērošanas pasākumu īstenošanu.[526]

Lietā "La Quadrature du Net u. c.", kurā EST noteica, ka izņēmuma gadījumā var paredzēt visaptverošus un nediferencētus datu saglabāšanas pasākumus, tā arī norādīja, ka, ņemot vērā no tiem izrietošās iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās smagumu, ir jānodrošina, lai šo pasākumu izmantošana patiešām attiektos tikai uz situācijām, kurās pastāv nopietns apdraudējums valsts drošībai. Šajā ziņā ir būtiski, lai lēmumu, ar kuru elektronisko komunikāciju pakalpojumu sniedzējiem tiek uzdots veikt šādu datu saglabāšanu, varētu efektīvi kontrolēt vai nu tiesa, vai arī neatkarīga administratīva iestāde, kuras

524 EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15 .., 118., 119. punkts.

525 Turpat, 120. punkts un tajā minētā judikatūra. Sk. arī EST 2009. gada 7. maija spriedumu lietā C-553/07 *Rijkeboer*, ECLI:EU:C:2009:293, 52. punkts, EST 2015. gada 6. oktobra spriedumu lietā C-362/14, 95. punkts.

526 Sk., piemēram, EST 2020. gada 16. jūlija spriedumu lietā C-311/18, 179., 183. punkts.

lēmumam ir saistoša iedarbība, lai pārbaudītu, vai pastāv šāda situācija, kā arī – vai ir ievēroti paredzētie nosacījumi un garantijas.[527]

Tāpat EST minētajā lietā norādīja, ka ir būtiski, lai pasākuma, ar kuru atļauj reāllaikā vākt informāciju par datu plūsmu un atrašanās vietas datus, īstenošana būtu pakļauta iepriekšējai pārbaudei, ko veic tiesa vai neatkarīga administratīva iestāde, kuras lēmumam ir saistoša iedarbība, un ka šai tiesai vai šai iestādei turklāt ir jāpārliecinās, ka šāda vākšana reāllaikā tiek atļauta vienīgi absolūti nepieciešamā robežās. Pienācīgi pamatotos neatliekamības gadījumos pārbaude jāveic īsā laikā.[528]

Neatkarīgas uzraudzības iestādes kontrolei ir būtiska nozīme, lai pārbaudītu, vai pastāv situācija, kas pamato pasākumu piemērošanu, un vai ir ievēroti nosacījumi un aizsardzības garantijas. Neatkarīgam uzraudzības mehānismam ir jābūt izveidotam, arī lai kontrolētu mākslīgā intelekta novērošanas pasākumus. Līdzās neatkarīgam uzraudzības mehānismam ir jābūt pieejamiem arī efektīviem tiesību aizsardzības līdzekļiem.

5.3.4. Efektīvi tiesību aizsardzības līdzekļi

Pēdējā būtiskā garantija ir saistīta ar tiesībām uz efektīviem tiesiskās aizsardzības līdzekļiem, lai aizsargātu personas tiesības, ja viņa uzskata, ka tās netiek ievērotas. Minētās tiesības ir noteiktas Hartas 47. pantā, kura pirmā daļa paredz, ka ikvienai personai, kuras tiesības un brīvības, kas garantētas ES tiesībās, tikušas pārkāptas, ir tiesības uz efektīvu tiesību aizsardzību tiesā. Hartas 47. panta otrā daļa paredz ikvienas personas tiesības uz taisnīgu, atklātu un laikus veiktu lietas izskatīšanu neatkarīgā un objektīvā, tiesību aktos noteiktā tiesā. EST "Schrems I" lietā vērš uzmanību, ka tiesiskai valstij ir raksturīga pārbaude tiesā, un tās mērķis ir nodrošināt ES tiesību normu ievērošanu. Tiesiskajā regulējumā, kurā indivīdiem nav paredzētas nekādas iespējas izmantot tiesību aizsardzības līdzekļus, lai piekļūtu personas datiem, kas uz tiem attiecas, vai panāktu šādu datu labošanu vai dzēšanu, nav ņemta vērā Hartas 47. pantā paredzēto pamattiesību uz efektīvu aizsardzību tiesā būtība.[529]

Efektīvu tiesību aizsardzība ir nesaraujami saistīta ar tiesībām uz informāciju. Lai personas varētu aizstāvēt savas tiesības, viņām ir jāpaziņo par novērošanas pasākumu piemērošanu pēc novērošanas pasākuma pabeigšanas. EST lietā "Tele 2 Sverige AB" norāda – ir būtiski, ka kompetentās valsts iestādes, kurām ir piešķirta piekļuve saglabātajiem datiem, par to informē attiecīgās personas

527 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 139. punkts.

528 Turpat, 189. punkts.

529 EST 2015. gada 6. oktobra spriedums lietā C-362/14, 95. punkts.

atbilstoši piemērojamajām valsts procesuālajām normām no brīža, kad šī saziņa vairs nevar traucēt šo iestāžu veiktajai izmeklēšanai. Proti, šī informēšana faktiski ir nepieciešama, lai ļautu šīm personām to tiesību pārkāpuma gadījumā īstenot tiesības uz tiesisko aizsardzību.[530]

Lietā "La Quadrature du Net u. c." EST norāda, ka ir būtiski, lai kompetentās valsts iestādes, kuras veic informācijas par datu plūsmu un atrašanās vietas datu vākšanu reāllaikā, par to informētu datu subjektus atbilstoši piemērojamajām valsts procesuālajām normām tiktāl un no brīža, kad šī informēšana vairs nevar traucēt šo iestāžu uzdevumu izpildi. Šī informēšana faktiski ir nepieciešama, lai ļautu šīm personām īstenot to tiesības, kas izriet no Hartas 7. un 8. panta, lūgt piekļuvi saviem personas datiem, kas ir šo pasākumu priekšmets, un vajadzības gadījumā panāktu to labošanu vai dzēšanu, kā arī saskaņā ar Hartas 47. panta pirmo daļu izmantotu tiesības uz efektīvu tiesību aizsardzību tiesā.[531] Attiecībā uz informēšanu, kas tiek prasīta informācijas par datu plūsmu un atrašanās vietas datu automatizētas analīzes kontekstā, jānorāda, ka kompetentajai valsts iestādei ir jāpublicē vispārēja rakstura informācija par šo analīzi, taču tai nav pienākuma individuāli informēt datu subjektus. Savukārt gadījumā, ja dati atbilst pasākumā, ar ko atļauta automatizētā analīze, precizētajiem parametriem un ja kompetentā valsts iestāde identificē datu subjektu, lai padziļināti analizētu datus, kas uz viņu attiecas, ir nepieciešams šo personu informēt individuāli. Tomēr šāda informācija ir jāsniedz tikai un vienīgi tādā apmērā un no tā brīža, kad tā nevar apdraudēt minētajai iestādei uzticēto uzdevumu izpildi.[532]

Tomēr EST lietā "La Quadrature du Net u. c." nesniedz norādes, vai izņēmuma gadījumā, kad pastāv nopietni draudi valsts drošībai un preventīvi ir paredzēta informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana, būtu jāinformē par to personas. EST vienīgi vispārīgi norāda, ka attiecīgo datu saglabāšanai jānotiek atbilstoši tai paredzētajiem materiāltiesiskajiem un procesuālajiem nosacījumiem un ka datu subjektiem ir efektīvas garantijas pret ļaunprātīgas izmantošanas risku.[533]

Kā uzsvērusi arī ECT, lai persona varētu efektīvi izmantot tiesību aizsardzības līdzekļus, tai ir jābūt informētai par pasākumiem, kas tiek veikti pret viņu. Veicot slepenu novērošanu, pēc tās beigām persona ir jāinformē par pret viņu veiktajiem pasākumiem. Personai principā ir maz iespēju vērsties tiesā, ja vien viņa nav informēta par pasākumu veikšanu bez viņa ziņas, un tad šī persona ar atpakaļejošu spēku var apstrīdēt to likumību, vai arī persona var vērsties tiesā,

530 EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15, 121. punkts.

531 EST 2020. gada 6. oktobra spriedums apvienotajās lietās C-511/18 .., 190. punkts.

532 Turpat, 191. punkts.

533 Turpat, 168. punkts.

ja tai ir aizdomas, ka viņa saziņa tiek vai ir pārtverta.[534] Tajā pašā laikā lietā "Big Brother Watch u. c. pret Apvienoto Karalisti" ECT atzīst, ka prasība pēc "turpmākas paziņošanas" paredz skaidri definētu novērošanas mērķu esamību, kas vienkārši nenotiek lielapjoma jeb masveida datu pārtveršanas režīmā.[535]

Ikvienas personas tiesības efektīvi aizstāvēt savas tiesības ir būtiskas, ja pret personu tiek piemēroti masveida novērošanas pasākumi, it īpaši, ja tie šo personu skar tieši un ietekmē lēmumu pieņemšanu pret personu, piemēram, aizturēšanu. Vienlaicīgi, lai tiktu nodrošinātas efektīvas garantijas pret uzraudzības pilnvaru ļaunprātīgu izmantošanu, turklāt ņemot vērā ierobežotās iespējas katrai atsevišķai personai aizstāvēt savas tiesības, būtiska nozīme ir nevalstisko un tiesību aizsardzības organizāciju darbībai. Kā jau iepriekš norādīts, ECT masveida novērošanas lietās pieņem arī kolektīvās sūdzības. Piemēram, ECT "Big Brother Watch u. c. pret Apvienoto Karalisti" lietā pieteicēji bija vairāk nekā desmit nevalstiskās un tiesību aizstāvības organizācijas.[536] Pilsoniskā līdzdalība ir būtiska garantija, lai uzraudzītu valsts piemēroto pasākumu likumību un novērstu varas ļaunprātīgu izmantošanu.

Nodaļā apskatītā ECT un EST tiesu prakse apstiprina, ka masveida novērošanas pasākumi rada būtisku iejaukšanos privātumā un datu aizsardzībā. Kā visbūtiskākais nosacījums, piemērojot masveida novērošanas pasākumus, ir norādīts pienākums izvērtēt, vai piemērotie pasākumi ir "stingri" jeb "absolūti" nepieciešami konkrētā mērķa sasniegšanai un vai tie ir samērīgi jeb proporcionāli ar šo mērķi. Visās lietās ir uzsvērta nepieciešamība tiesību aktos noteikt atbilstošas procesuālās garantijas, it īpaši tiesas vai neatkarīgas iestādes kontroli un pienākumu informēt personas par šādu pasākumu piemērošanu.

Šos nosacījumus ir būtiski ievērot arī pirms jaunu novērošanas tehnoloģiju ieviešanas. Vairāki gadījumi attiecībā uz sejas atpazīšanas tehnoloģiju piemērošanu liecina, ka praksē bieži vien tās tiek ieviestas, neizvērtējot, vai tas ir "stingri" jeb "absolūti" nepieciešams un vai tas ir samērīgi, kā arī tās tiek izmantotas slepeni, neinformējot personas un sabiedrību.[537] Lai izvērtētu novērošanas pasākumu nepieciešamību, ir jāizvērtē šo pasākumu piemērotība un efektivitāte, lai sasniegtu mērķi, un jāizvērtē, vai ir izvēlēts vismazāk aizskarošs līdzeklis. Tajā pašā laikā to izdarīt ir ļoti problemātiski, jo trūkst empīrisko pierādījumu par

534 ECT 2015. gada 4. decembra spriedums lietā 47143/06, 234. punkts; ECT 1978. gada 6. septembra spriedums lietā 5029/71, 57. punkts; ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13 .., 310. punkts.

535 ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13 .., 317. punkts.

536 Sk. ECT 2018. gada 13. septembra spriedumu apvienotajās lietās 58170/13 .., Appendix. List of Applicants.

537 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

šādu pasākumu efektivitāti.[538] Nav pieļaujams, ka masveida novērošanas pasākumi, kas būtiski ierobežo personu pamattiesības, to skaitā tādi, kas izmanto jaunās novērošanas tehnoloģijas, tiek ieviesti un piemēroti, neizvērtējot to proporcionalitāti un nepieciešamību, nenodrošinot atbilstošas procesuālas garantijas un it īpaši – neinformējot personas. Šāda prakse neatbilst tiesiskas valsts principa prasībām un var apdraudēt demokrātiju.

Plašā EST un ECT prakse sniedz būtiskas vadlīnijas, kā izvērtēt, vai plānotie vai esošie novērošanas pasākumi ir atbilstoši tiesību uz privātumu un datu aizsardzību ierobežošanas nosacījumiem. Tajā pašā laikā ir svarīgi, lai Hartas 8. pantā noteiktās tiesības uz personas datu aizsardzību garantētu plašu aizsardzību, kas ietver ne tikai šī panta 2. un 3. punktā tieši paredzētās garantijas, bet arī citus būtiskus datu aizsardzības principus un garantijas, kas noteiktas galvenajos ES datu aizsardzības tiesību aktos.[539] Hartas 8. panta 2. punkts nosaka personas datu apstrādes nosacījumus, proti, šādi dati ir jāapstrādā godprātīgi, noteiktiem mērķiem un ar likumīgu pamatojumu, kas paredzēts tiesību aktos. Harta arī paredz, ka ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un ir tiesības ieviest labojumus šajos datos. Hartas 8. panta 3. punkts savukārt paredz, ka atbilstību šiem noteikumiem ir jākontrolē neatkarīgai iestādei. EST bieži ir atsaukusies uz šajās normās noteiktajām garantijām. Tajā pašā laikā masveida novērošanas pasākumiem ir jāatbilst dažādiem principiem un prasībām, kas paredzētas VDAR un citos datu aizsardzības tiesību aktos. Šīs prasības aplūkotas nākamajā grāmatas nodaļā.

538 Sk. Tzanou (2019), *The Fundamental Right to Data Protection*, p. 253.

539 Ibid., p. 255.

6. DAĻA

Datu aizsardzības pamatprasības mākslīgā intelekta novērošanas tehnoloģijām

Datu aizsardzības tiesības ir galvenais regulējums, kas jau šobrīd ir piemērojams attiecībā uz mākslīgo intelekta sistēmu izstrādi, ieviešanu un izmantošanu, tiklīdz tās skar personas datu apstrādi. Datu aizsardzības regulējums palīdz novērst radīto apdraudējumu ne tikai tiesībām uz privātumu un datu aizsardzību, bet arī citām pamattiesībām, piemēram, diskriminācijas aizlieguma principam. Kā tika atklāts iepriekšējā nodaļā, tas lielā mērā ietekmē un uz to ir balstīta mākslīgā intelekta regulējuma turpmākā attīstība. Jautājums ir, ciktāl Eiropā pastāvošais datu aizsardzības regulējums var palīdzēt novērst mākslīgā intelekta novērošanas sistēmu radītos riskus cilvēktiesībām un nodrošināt to atbildīgu izstrādi, ieviešanu un izmantošanu. Vai datu aizsardzības regulējums ir pietiekams, vai arī gluži pretēji – būtu nepieciešams speciāls regulējums attiecībā uz noteiktiem mākslīgā intelekta izmantošanas veidiem, nosakot jaunas prasības un ierobežojumus?

Datu aizsardzības regulējums izvirza daudzas prasības mākslīgā intelekta un cita veida novērošanas tehnoloģijām un paredz speciālus noteikumus attiecībā uz biometrisko datu apstrādi. Šajā nodaļā izvērtētas būtiskākās datu aizsardzības prasības, kas ir piemērojamas mākslīgā intelekta novērošanas pasākumiem, un vērsta uzmanība uz galvenajiem problēmjautājumiem, īpašu uzmanību veltot sejas atpazīšanas tehnoloģijām. Nodaļā aplūkoti un salīdzināti noteikumi, kas ietverti VDAR, kura paredz vispārējās prasības, un Policijas direktīvā, kura ir piemērojama attiecībā uz tiesībaizsardzības iestādēm, kā arī Konvencijā 108+ ietvertās normas, kuras vērš uzmanību uz kopīgajām un atšķirīgajām garantijām. Nodaļas nobeigumā atsevišķi aplūkoti datu aizsardzības standarti, kas ietverti starptautisko organizāciju izdotajās rekomendācijās kontaktu izsekošanas lietotnēm, un būtiskie izaicinājumi to piemērošanā praksē, vēršot uzmanību uz nepieciešamību minētos standartus attiecināt arī uz mākslīgā intelekta novērošanas tehnoloģijām.

6.1. Personas datu apstrāde un biometriskā novērošana

Datu aizsardzības tiesību centrālais elements ir personas datu jēdziens, kas nosaka datu aizsardzības tiesību aktu materiālo piemērošanu.

VDAR un Policijas direktīvā ir sniegta vienāda personas datu definīcija: “Personas dati ir jebkura informācija, kas attiecas uz identificētu vai identificējamu

fizisku personu ("datu subjektu"); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, it īpaši, atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem." (VDAR 4. panta 1. punkts, Policijas direktīvas 3. panta 1. punkts). Konvencija 108+ personas datus definē īsāk, kā "jebkuru informāciju, kas attiecas uz identificētu vai identificējamu personu (datu subjektu)" (2. panta a) punkts).

Par personas datiem netiek uzskatīta informācija, kas, lai gan attiecas uz cilvēkiem, neattiecas uz konkrētu personu. Lai šādu informāciju atzītu par personas datiem, personai ir jābūt "identificētai vai identificējamai". Persona ir identificējama, ja tā vēl nav identificēta, bet to ir iespējams identificēt. Lai noteiktu, vai fizisku personu ir iespējams identificēt, ir jāņem vērā visi līdzekļi, ko varētu izmantot, piemēram, atsevišķa izdalīšana, lai tieši vai netieši identificētu fizisku personu (VDAR 26. apsvērums).

Gan VDAR, gan Policijas direktīva atsevišķi izdala īpašu kategoriju personas datus, kuriem paredzēta augstāka aizsardzība. Abi tiesību akti skaidro, ka tie ir tādi personas dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, ģenētiskie dati, biometriskie dati, kas ļauj veikt fiziskas personas unikālu identifikāciju, veselības dati un dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju (VDAR 9. panta 1. punkts, Policijas direktīvas 10. pants). Konvencijas 108+ 6. pants paredz, ka īpašu kategoriju datu apstrāde ietver: ģenētisko datu apstrādi; personas datus, kas attiecas uz noziedzīgiem nodarījumiem, kriminālprocesiem, notiesājošiem spriedumiem un saistītiem drošības pasākumiem; biometriskos datus, kas unikāli identificē personu; personas datus attiecībā uz informāciju, ko tie atklāj, saistībā ar rasi vai etnisko izcelsmi, politiskajiem uzskatiem, dalību arodbiedrībās, reliģisko vai citu pārliecību, veselību vai seksuālo dzīvi.

Gan VDAR, gan Policijas direktīva sniedz arī identisku biometrisko datu definīciju: "Biometriskie dati ir personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprina minētās fiziskās personas unikālu identifikāciju, piemēram, sejas attēli vai daktiloskopijas dati." (VDAR 4. panta 14. punkts, Policijas direktīvas 3. panta 13. punkts.)

ES datu aizsardzības regulējumā biometrisko datu definīcija ir formulēta plaši, lai tā aptvertu fiziskās, fizioloģiskās vai uzvedības pazīmes. Par biometriskiem datiem ir atzītas dažādas informācijas kategorijas: tās var būt "fiziskās / fizioloģiskās īpašības" (piemēram, sejas vaibsti, pirkstu nospiedumi), bioķīmiskas pazīmes (DNS), kā arī motorika vai dažādi uzvedības raksturlielumi (ieradumi, personības

iezīmes, atkarības, gaita, taustiņu nospiešanas veids utt.).[540] Digitālie sejas attēli pieder pie pirmās kategorijas, vienlaicīgi, ja tiek izmantotas, piemēram, emocionālās uztveršanas sistēmas, tie var atklāt arī dažādas personības iezīmes.

Cilvēka sejas attēls ir uzskatāms par biometriskajiem datiem. Tas ir vairāk vai mazāk unikāls, kā arī tas maz mainās. To parasti nevar noslēpt, lai gan Covid-19 pandēmijas laikā sejas bieži aizsedza maskas. Sejas attēlu ir arī viegli iegūt, jo atšķirībā no DNS vai pirkstu nospiedumu iegūšanas procesa personai parasti ir grūti izvairīties no tās publiskas novērošanas.[541] Tajā pašā laikā sejas attēlu apstrādes konteksts ir būtisks, lai noteiktu datu sensitīvo raksturu, jo ne visa attēlu apstrāde ietver īpašu kategoriju personas datu apstrādi. Uz attēliem biometrisko datu definīcija attieksies tikai tad, ja tos apstrādā, izmantojot īpašu tehnisku līdzekli, kas ļauj unikāli identificēt vai autentificēt personu.[542] VDAR skaidro, ka fotogrāfiju apstrāde nebūtu vienmēr jāuzskata par īpašu kategoriju personas datu apstrādi, jo uz tām biometrisko datu definīcija attiecas tikai tad, kad tās apstrādās ar konkrētiem tehniskiem līdzekļiem, kas ļauj veikt fiziskas personas unikālu identifikāciju vai autentifikāciju (51. apsvērums).

Eiropas Datu aizsardzības kolēģija ir norādījusi, ka personas videomateriālu nevar uzskatīt par biometriskiem datiem saskaņā ar VDAR 9. pantu, ja tas nav īpaši tehniski apstrādāts, lai veicinātu personas identificēšanu. Lai to varētu uzskatīt par īpašu kategoriju personas datu apstrādi (9. pants), biometriskie dati ir jāapstrādā "fiziskas personas unikālas identificēšanas nolūkā". Ievērojot VDAR 4. panta 14. punktu un 9. pantu, jāņem vērā trīs kritēriji:

1) datu veids – dati par fiziskas personas fiziskām, fizioloģiskām vai uzvedības īpašībām;
2) apstrādes līdzekļi un veids – dati, kas iegūti "īpašā tehniskā apstrādē";
3) apstrādes mērķis – dati jāizmanto, lai unikāli identificētu fizisku personu.[543]

Biometriskie dati, kā tie ir definēti VDAR 4. panta 14. punktā un Policijas direktīvas 3. panta 13. punktā, ir personas datu apakškategorija, līdz ar to tiem ir jāatbilst šajos pantos minētajiem kritērijiem. Tas, cik lielā mērā biometriskās shēmas var uzskatīt par personas datiem, ir ilgstošu diskusiju temats.

Biometrisko sistēmu mērķis parasti ir personas identificēšana (personas identifikācija salīdzinājumā ar citu personu) vai personas autentifikācija, kas

540 Article 29 Data Protection Working Party. (2012). Opinion 3/2012 on developments in biometric technologies. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

541 FRA (2019), Facial recognition technology.

542 Council of Europe (2021), .. Convention 108.

543 EDPB. (2020). Guidelines 3/2019 on processing of personal data through video devices. Version 2.0. Adopted on 29 January 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

tiek saukta arī par verifikāciju (noteikšana, vai persona ir tā, par ko tā izliekas).[544] Abus jēdzienus ir skaidrojusi 29. panta darba grupa, kas norāda, ka "personas identificēšana, izmantojot biometrisko sistēmu, parasti ir process, kurā tiek salīdzināti indivīda biometriskie dati (kas iegūti identifikācijas brīdī) ar vairākām datubāzē glabātām biometriskām veidnēm (t. i., salīdzināšanas process "viens pret daudziem")", savukārt "personas verifikācija, izmantojot biometrisko sistēmu, parasti ir process, kurā salīdzina indivīda biometriskos datus (kas iegūti verifikācijas laikā) ar vienu biometrisko veidni, kas glabājas ierīcē (t. i., viens pret vienu salīdzināšanas process)".[545]

Biometrisko datu definīcija, liekas, aptver abus veidus, paredzot, ka tie "ļauj veikt vai apstiprina personas unikālu identifikāciju" (VDAR 4. panta 14. punkts; Policijas direktīvas 3. panta 13. punkts). Arī VDAR 51. pantā ir norādīts "ļauj veikt fiziskas personas unikālu identifikāciju". Tomēr šie dažādie mērķi netiek atkārtoti VDAR 9. panta 1. punktā un Policijas direktīvas 10. pantā, kas attiecībā uz personas datiem ir ierobežoti ar gadījumiem, kad dati tiek apstrādāti, lai veiktu fiziskas personas unikālu identifikāciju. Proti, VDAR 9. panta 1. punkts un Policijas direktīvas 10. pants ir attiecināms tikai uz biometriskajiem datiem, kas tiek izmantoti personas unikālai identifikācijai, bet ne autentifikācijai.[546]

FRA sejas atpazīšanas izmantošanu iedala trīs veidos: verifikācijai, identifikācijai un kategorizācijai.[547] Verifikācijas procedūru izmanto, piemēram, automatizētai robežkontrolei lidostu pārbaudēs. Persona ieskenē savu pases attēlu, un uz vietas tiek uzņemts attēls. Sejas atpazīšanas tehnoloģija salīdzina abus sejas attēlus, un, ja varbūtība, ka abi attēli parāda vienu un to pašu personu, pārsniedz noteiktu varbūtības slieksni, tiek apstiprināta identitāte. Pārbaude neprasa, lai biometriskās pazīmes tiktu glabātas centrālajā datubāzē. Tos var uzglabāt, piemēram, personas identitāti apliecinošā vai ceļošanas dokumentā.

Tiek uzskatīts, ka biometrisko datu izmantošana identifikācijai rada daudz lielāku apdraudējumu (tai skaitā no datu aizsardzības viedokļa), nekā to izmantošana autentifikācijai jeb verifikācijai. Sejas atpazīšanas tehnoloģijas tiek izmantotas personas identifikācijai, ja personas sejas attēls tiek salīdzināts ar daudziem citiem attēliem, kas glabājas datubāzē, lai uzzinātu, vai šī persona ir iekļauta konkrētajā datubāzē. Katram salīdzinājumam tiek dots konkrēts punktu skaits, norādot varbūtību, ka divi attēli attiecas uz vienu un to pašu personu. Dažreiz attēlus pārbauda, salīdzinot ar datubāzēm, kur ir zināms, ka persona, kuras attēls

544 Kuner, C., Bygrave, L. A., Docksey, C. (eds.). (2019). *The EU General Data Protection Regulation* (*GDPR*): *A Commentary*. Oxford, United Kingdom: Oxford University Press, p. 213.

545 Article 29 Data Protection Working Party (2012), Opinion 3/2012 ..

546 Kuner, Bygrave, Docksey (2019), *The EU General Data Protection Regulation* .., p. 214.

547 FRA (2019), Facial recognition technology.

tiek salīdzināts, atrodas datubāzē (slēgta datu kopas identifikācija), un dažreiz, – ja tas nav zināms (atvērta datus kopas identifikācija). Pēdējā darbība ir piemērota, ja personas tiek pārbaudītas pēc novērošanas sarakstiem. Sejas atpazīšanas tehnoloģijas izmantošanu identifikācijai dažkārt sauc par automatizētu sejas atpazīšanu.

Identifikāciju var veikt, izmantojot sejas attēlus, kas iegūti no videokamerām. Sejas attēli arī videomateriālos tiek iegūti un pēc tam salīdzināti ar sejas attēliem datubāzē, lai identificētu, vai videomateriālā redzamā persona ir atrodama attēlu datubāzē (meklējamo personu sarakstā). Ar videokamerām iegūto sejas attēlu kvalitāti nevar kontrolēt: gaisma, attālums un atrašanās vieta ierobežo videomateriālos uzņemtās personas sejas vaibstus. Tāpēc sejas atpazīšanas tehnoloģiju izmantošana, visticamāk, rada nepatiesas atbilstības salīdzinājumā ar sejas attēliem, kas uzņemti kontrolētā vidē, piemēram, robežas šķērsošanas vietā vai policijas iecirknī.

Sejas atpazīšanas tehnoloģijas tiek izmantota arī kategorizācijai.[548] Sejas attēlu var analizēt, kā arī var veikt tā saucamo emociju, uzvedības jeb afektīvo analīzi. To var izmantot arī indivīdu profilēšanai, kas ietver indivīdu kategorizāciju, pamatojoties uz viņu personīgajām īpašībām.[549] Pēc sejas attēliem parasti nosakāmās īpašības ir dzimums, vecums un etniskā izcelsme. Sejas atpazīšanas tehnoloģijas tiek izmantotas, lai atpazītu cilvēku emocijas, piemēram, dusmas, bailes vai laimes sajūtu, un lai noteiktu, vai cilvēki melo vai saka patiesību. Ir bijuši eksperimenti, izmantojot sejas attēlu, noteikt personas seksuālo orientāciju. Kategorizācijas gadījumā šīs tehnoloģijas netiek izmantotas indivīdu identifikācijai, bet gan indivīda raksturošanai, bet tas ne vienmēr ļauj personu identificēt. Tomēr, ja no sejas tiek secināti vairāki raksturlielumi un tie, iespējams, ir saistīti ar citiem datiem (piemēram, atrašanās vietas datiem), tas faktiski varētu ļaut identificēt personu.[550]

Profesors Dž. Sartors vērš uzmanību, ka mākslīgais intelekts izvirza jautājumus, kas saistīti ar personas datu būtību, it sevišķi attiecībā uz iespēju secināt jaunus personas datus no esošajiem datiem, kā arī iespēju atkal savienot datu subjektus ar viņu identificētajiem datiem. Šajā saistībā personas datu jēdziens, kas noteikts ES datu aizsardzības tiesību aktos, nesniedz skaidras atbildes. Zinātnieks

548 MI akta priekšlikums definē "biometriskās kategorizācijas sistēmu" kā mākslīgā intelekta sistēmu, kuras mērķis ir noteikt fizisku personu piederību noteiktām kategorijām, piemēram, tādām kā dzimums, vecums, matu krāsa, acu krāsa, tetovējumi, etniskā izcelsme vai seksuālā vai politiskā orientācija, pamatojoties uz viņu biometriskajiem datiem (1. panta 35. punkts); Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

549 Sk. FRA. (2018). Preventing unlawful profiling today and in the future: a guide. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

550 FRA (2019), Facial recognition technology.

uzskata, ka par personas datiem ir jāatzīst arī tā sauktie izsecināmie personas dati. Viņš norāda, ka mākslīgā intelekta algoritmi var izsecināt jaunu informāciju par datu subjektiem, viņu personas datiem.

No datu aizsardzības viedokļa galvenais jautājums ir, vai secinātā informācija būtu jāuzskata par jauniem personas datiem un vai tā ir nodalāma no datiem, no kuriem tā ir izsecināta. Pieņemsim, ka, piemēram, indivīda seksuālā orientācija tiek izsecināta no viņa sejas vai sejas īpašībām, vai no šīs personas aktivitātēm tiešsaistē. Vai izsecinātais seksuālās orientācijas vai personības veids būtu jauns personas datu elements? Pat tad, ja secinājums ir tikai varbūtīgs? Ja izsecinātā informācija tiek uzskatīta par jauniem personas datiem, tad attiecībā uz šādiem automatizētiem secinājumiem rastos pienākums ievērot visas prasības, kuras saskaņā ar datu aizsardzības noteikumiem ir noteiktas personas datu apstrādei: tiesiskā pamata nepieciešamību, nosacījumus sensitīvu datu apstrādei, datu subjekta tiesības utt. Iespējamā pieeja varētu būt to gadījumu nošķiršana, kuros personas datu izsecināšana tiek veikta, neveicot citas darbības, t. i., izsecinātie personas dati ir tikai aprēķina rezultāts, no kuriem neizriet tālākas darbības, atšķirībā no tiem gadījumiem, kad secināmos datus izmanto, lai veiktu novērtējumu un pieņemtu lēmumus. Pēdējā gadījumā dati noteikti būtu jāuzskata par jaunievāktiem personas datiem. [551]

Mākslīgā intelekta sistēmas palielina acīmredzami anonīmu datu identificējamību, jo tie ļauj neidentificētus datus, ieskaitot datus, kas ir anonimizēti vai pseidonimizēti[552], saistīt ar attiecīgajām personām. VDAR 26. apsvērumā un Policijas direktīvas 21. apsvērumā ir norādīts, ka "datu aizsardzības principi nebūtu jāpiemēro anonīmai informācijai, proti, informācijai, kura neattiecas uz identificētu vai identificējamu fizisku personu, vai personas datiem, ko sniedz anonīmi tādā veidā, ka datu subjekts nav vai vairs nav identificējams". Dž. Sartors norāda, ka būtu ieteicams precizēt, iespējams, nesaistošā tiesību aktā vai atzinumā, ka atkārtota identifikācija ir personas datu apstrāde un to patiešām var pielīdzināt jaunu personas datu vākšanai. Tāpēc uz atkārtotu identifikāciju pilnībā attiecas visas VDAR prasības, tostarp pienākums informēt datu subjektu un nepieciešamība pēc tiesiskā pamata.[553]

551 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

552 Pseidonimizācija ir personas datu apstrāde, ko veic tādā veidā, lai personas datus vairs nav iespējams saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka personas dati netiek saistīti ar identificētu vai identificējamu fizisku personu (VDAR 4. panta 5. punkts). VDAR 28. apsvērums paredz, ka personas dati, kuri ir pseidonimizēti un kurus, izmantojot papildu informāciju, varētu attiecināt uz fizisku personu, ir uzskatāmi par informāciju par identificējamu fizisku personu.

553 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

Īpašu kategoriju personas datu apstrāde, to skaitā biometrisko datu apstrāde, var radīt nopietnu risku pamattiesībām un brīvībām, tāpēc tiem ir noteikta īpaša aizsardzība (Policijas direktīvas 37. apsvērums, VDAR 51. apsvērums). VDAR aizliedz īpašu kategoriju datu apstrādi, ja vien nepastāv kāds no VDAR konkrēti paredzētiem pamatojumiem. Policijas direktīva un Konvencija 108+ atļauj šādu datu apstrādi, ja tiek ievēroti stingri nosacījumi, kas aplūkoti nākamajā apakšnodaļā.

6.2. Personas datu apstrādes pamatprincipi

Personas datu apstrādes principi ir pamatā un jāpiemēro, interpretējot pārējās datu aizsardzības prasības. Pamatprincipi, kas tika ietverti, piemēram, 1981. gada Konvencijā 108, nav būtiski mainījušies, ja tos salīdzina ar citām datu aizsardzības prasībām, kas ir attīstījušās vairākus gadsimtus. Tie ir izturējuši laika pārbaudi un var tikt piemēroti dažādos tehniskos, ekonomiskos un sociālos kontekstos.[554] Datu aizsardzības principi ir piemērojami arī mākslīgā intelekta tehnoloģijām. VDAR 5. pants nosaka šādus personas datu apstrādes principus: likumīgums, godprātība un pārredzamība, nolūka ierobežojums, datu minimizēšana, precizitāte, glabāšanas ierobežojums, integritāte un konfidencialitāte, pārskatatbildība. Policijas direktīvas 4. pants paredz gandrīz visus tos pašus principus, izņemot pārredzamības un pārskatatbildības principu. Daži no principiem ir tālāk attīstīti turpmākajos pantos, piemēram, likumības princips, kas noteikts VDAR 5. panta 1. punkta a) apakšpunktā un Policijas direktīvas 4. panta 1. punkta a) apakšpunktā, ir tālāk skaidrots VDAR 6. pantā un Policijas direktīvas 8. pantā.

6.2.1. Likumīgums, tiesiskais pamats un nolūka ierobežojuma princips

VDAR kā pirmos principus paredz, ka personas dati tiek apstrādāti likumīgi, godprātīgi un datu subjektiem pārredzamā veidā (5. panta 1. punkta a) apakšpunkts). Policijas direktīva nosaka, ka personas dati tiek apstrādāti likumīgi un godprātīgi (4. panta 1. punkta a) apakšpunkts). Arī Konvencijā 108+ ir noteikts, ka personas datus apstrādā likumīgi (5. panta 3. punkts).

No likumīguma principa izriet vispārējs nosacījums, ka personas dati jāapstrādā, ievērojot tiesību aktos noteiktās prasības. Saskaņā ar VDAR un Policijas direktīvu likumīguma princips paredz, ka datu apstrādei, lai tā būtu likumīga, ir jābūt tiesiskam pamatam. VDAR 6. panta 1. punkts paredz, ka personas datu

554 Kuner, Bygrave, Docksey (2019), *The EU General Data Protection Regulation* .., p. 311.

apstrāde ir likumīga tikai tādā apmērā un tikai tad, ja tai ir piemērojams viens no turpmāk minētajiem pamatojumiem:

1) piekrišana;
2) līguma izpilde;
3) juridiskais pienākums;
4) personas vitālās intereses;
5) sabiedrības intereses un likumīgi piešķirtās oficiālās pilnvaras;
6) leģitīmas intereses.

Apstrādes likumīguma princips ir noteikts Policijas direktīvas 8. pantā. Tā 1. punkts paredz, ka apstrāde ir likumīga tikai tad un tiktāl, ciktāl šī apstrāde ir nepieciešama tā uzdevuma izpildei, ko kompetentā iestāde veic 1. panta 1. punktā minētajos nolūkos (proti, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu), un ka tā balstās uz ES vai dalībvalsts tiesībām. Policijas direktīvas 8. panta 2. punkts savukārt paredz, ka dalībvalsts tiesībās, ar ko regulē apstrādi šīs direktīvas darbības jomā, precizē vismaz apstrādes mērķus, apstrādājamos personas datus un apstrādes nolūkus.

Līdzīgi Konvencijas 108+ 5. panta 2. punkts nosaka, ka datu apstrādei jābūt tiesiskajam pamatam: "[k]atra Puse nodrošina, ka datu apstrādi var veikt, pamatojoties uz datu subjekta brīvu, specifisku, informētu un nepārprotamu piekrišanu vai kādu citu tiesisku pamatu, kas noteikts likumā."

VDAR aizliedz biometrisko datu kā īpašas kategorijas personas datu apstrādi, izņemot, ja pastāv kāds no 9. panta 2. punktā noteiktajiem gadījumiem. Šāda atkāpe, piemēram, ir pieļaujama, ja datu subjekts dot nepārprotamu piekrišanu (9. panta 1. punkta a) apakšpunkts). Piekrišanai ir jābūt ne tikai iegūtai atbilstošā veidā, bet tai ir jāatbilst visiem Regulā noteiktiem kritērijiem, proti, tai ir jābūt: brīvai, konkrētai, apzinātai un viennozīmīgai (4. panta 11. punkts).[555] Eiropas Padome Vadlīnijās par sejas atpazīšanu norāda, ka, ņemot vērā prasību pēc šādas datu subjektu piekrišanas, sejas atpazīšanas tehnoloģijas var izmantot tikai kontrolētā vidē verifikācijas, autentifikācijas vai kategorizācijas nolūkos. Biometriskā kategorizācija nozīmē procesu, lai noteiktu, vai indivīda biometriskie dati pieder grupai ar kādām iepriekš definētām īpašībām, un lai veiktu konkrētu darbību. Atkarībā no mērķa īpaša uzmanība jāpievērš datu subjekta "nepārprotamas piekrišanas" kvalitātei, ja tā ir apstrādes tiesiskais pamats.

Lai nodrošinātu brīvu piekrišanu, datu subjektiem jāpiedāvā alternatīvi risinājumi sejas atpazīšanas tehnoloģiju izmantošanai (piemēram, izmantot paroli

555 Sk. Article 29 Data Protection Working Party. (2017). Guidelines on Consent under Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/623051/en

vai identifikācijas zīmi). Turklāt, lai izvēle būtu īsta, tiem ir jābūt viegli izmantojamiem salīdzinājumā ar sejas atpazīšanas tehnoloģiju. Līdzīgi arī Eiropas Datu aizsardzības kolēģija ir uzsvērusi, ka gadījumos, kad piekrišana ir nepieciešama, pārzinis nevar ierobežot piekļuvi saviem pakalpojumiem atkarībā no piekrišanas biometriskai apstrādei, un, ja šādu apstrādi izmanto autentifikācijas nolūkā, datu pārzinim jāpiedāvā alternatīvs risinājums, kas neietver biometrisko apstrādi, – bez ierobežojumiem vai papildu izmaksām datu subjektam.[556]

Eiropas Padome uzsver, ka privātie uzņēmumi nevar izmantot sejas atpazīšanas tehnoloģijas nekontrolētā vidē, piemēram, tirdzniecības centros, it īpaši, lai identificētu interesējošas personas mārketinga vai drošības nolūkā. Iziešanu cauri telpai, kurā tiek izmantotas sejas atpazīšanas tehnoloģijas, nevar uzskatīt par nepārprotamu piekrišanu.[557]

Valsts iestādes nevar izmantot piekrišanu kā tiesisko pamatu, un tām ir atļauts apstrādāt biometriskos datus, ja apstrāde ir vajadzīga "būtisku sabiedrības interešu dēļ", pamatojoties uz ES vai dalībvalsts tiesību aktiem, ja tā ir samērīga ar izvirzīto mērķi, ievēro tiesību uz datu aizsardzību būtību un paredz piemērotus un konkrētus pasākumus datu subjekta pamattiesību un interešu aizsardzībai (VDAR 9. panta 2. punkta g) apakšpunkts).

Policijas direktīvas 10. pants savukārt paredz, ka īpašu kategoriju personas datu apstrāde ir atļauta tikai tad, kad tas ir absolūti nepieciešams, uz to attiecas atbilstošas garantijas attiecībā uz datu subjekta tiesībām un brīvībām, un:

a) tas ir atļauts ES vai dalībvalsts tiesībās;
b) lai aizsargātu datu subjekta vai citas fiziskas personas intereses; vai
c) šāda apstrāde attiecas uz datiem, kurus datu subjekts acīmredzami ir publiskojis.

Konvencija 108+ savukārt paredz, ka biometrisko datu apstrāde, kas unikāli identificē personas, ir atļauta, ja likumā ir paredzēti atbilstoši aizsardzības pasākumi, kas papildina Konvencijas nosacījumus. Šādi aizsardzības pasākumi novērš riskus, ko sensitīvu datu apstrāde var radīt datu subjekta interesēm, tiesībām un pamatbrīvībām, īpaši diskriminācijas risku.

Likumīguma princips un tiesiskā pamata piemērošana ir cieši saistīta ar tiesību uz datu apstrādes ierobežošanas nosacījumiem, kas noteikti, piemēram, Hartas 52. panta 1. punktā, proti, ka tiem ir jābūt paredzētiem likumā, tiem ir jābūt likumīgam mērķim, kā arī nepieciešamiem un proporcionāliem, lai sasniegtu šo mērķi. Konvencijas 108+ 5. pants nosaka datu apstrādes likumību (*legitimacy* – angļu val.) un datu kvalitātes principu. Minētā panta 1. punkts paredz: "Datu apstrāde ir proporcionāla izvirzītajam likumīgajam mērķim un visos apstrādes

556 EDPB (2019), Guidelines 3/2019 on processing of personal data through video devices.

557 Council of Europe (2021), .. Convention 108.

posmos atspoguļo taisnīgu līdzsvaru starp visām attiecīgajām interesēm – gan publiskām, gan privātām – un attiecīgajām tiesībām un brīvībām."

Eiropas Padome Vadlīnijās par sejas atpazīšanu uzsver, ka biometriskā datu apstrāde ar sejas atpazīšanas tehnoloģijām identifikācijas nolūkos kontrolētā vidē, kad biometriskās sistēmas var tikt izmantotas tikai ar personas līdzdalību, kā arī nekontrolētā vidē būtu jāattiecina tikai uz tiesībaizsardzības mērķiem. To drīkst veikt vienīgi kompetentās iestādes drošības jomā. Tiesību akti var paredzēt dažādus nepieciešamības un proporcionalitātes testus atkarībā no tā, vai to mērķis ir verifikācija vai identifikācija, ņemot vērā iespējamos riskus pamattiesībām un kamēr personu attēli tiek likumīgi vākti. Identifikācijas nolūkos ir jāievēro stingra nepieciešamība un proporcionalitāte gan datubāzes (novērošanas saraksta) izveidē, gan (reāllaika) sejas atpazīšanas tehnoloģiju ieviešanā nekontrolētā vidē. Tiesību aktos būtu jāparedz skaidri parametri un kritēriji, kas jāievēro tiesībaizsardzības iestādēm, veidojot datubāzes (novērošanas sarakstus) īpašiem, likumīgiem un nepārprotamiem tiesībaizsardzības mērķiem, piemēram, aizdomām par smagiem pārkāpumiem vai risku sabiedrības drošībai. Ņemot vērā šo tehnoloģiju aizskarošo raksturu, reāllaika sejas atpazīšanas tehnoloģiju ieviešanas posmā nekontrolētā vidē tiesību aktam ir jānodrošina, ka tiesībaizsardzības iestādes pierāda, ka dažādi faktori, tostarp šo tehnoloģiju ieviešanas vieta un laiks, attaisno lietošanas stingru nepieciešamību un proporcionalitāti.[558]

Eiropas Padome jau minētajās vadlīnijās arī pieļauj, ka sejas atpazīšanas tehnoloģijas var izmantot arī citām būtiskām sabiedrības interesēm valsts iestādes, kuru darbība nav saistīta ar tiesībaizsardzības mērķiem. Šādā gadījumā likumdevējiem un lēmumu pieņēmējiem ir jāpieņem īpaši noteikumi par biometrisko apstrādi, kas veikta, izmantojot sejas atpazīšanas tehnoloģijas. Likumdevējiem un lēmumu pieņēmējiem ir jānodrošina, ka nepārprotams un precīzs tiesiskais pamats garantē nepieciešamos aizsardzības pasākumus biometrisko datu apstrādei. Šādam tiesiskam pamatam ir jāietver stingra šo datu izmantošanas nepieciešamība un proporcionalitāte, kā arī jāņem vērā datu subjektu neaizsargātība un vide, kurā šīs tehnoloģijas tiek izmantotas verifikācijas nolūkos. Piemēram, sejas atpazīšanas tehnoloģiju izmantošanu drošības nolūkā kontrolētā vai nekontrolētā vidē, tostarp skolās vai citās sabiedriskās ēkās, parasti nevajadzētu uzskatīt par absolūti nepieciešamu un proporcionālu, ja pastāv mazāk uzmācīgi alternatīvi mehānismi.[559]

Eiropas Padome mudina pieņemt stingru tiesisko regulējumu sejas atpazīšanas tehnoloģiju izmantošanai, norādot arī gadījumus, kad tās nevar izmantot, piemēram, privātie uzņēmumi tās nedrīkstētu lietot nekontrolētā vidē. Tomēr

558 Council of Europe (2021), .. Convention 108.

559 Ibid.

valstīm tiek atstātas plašas iespējas regulēt šo tehnoloģiju izmantošanu publiskā sektorā, lemjot, kad tās būtu atzīstamas par absolūti nepieciešamām un proporcionālām, lai aizsargātu tādas būtiskas sabiedrības intereses kā noziedzīgu nodarījumu izmeklēšana, atklāšana un novēršana, sabiedrības drošība. Eiropas Padomei būtu jānosaka vēl skaidrāki ierobežojumi. Šis jautājums vairāk apskatīts nākamajā nodaļā.

Vēl viens problemātisks aspekts saistībā ar mākslīgā intelekta tehnoloģiju izmantošanu ir par datu, piemēram, fotoattēlu, kas vākti vienam nolūkam, izmantošanu citam nolūkam, piemēram, sejas atpazīšanas datubāzes veidošanai. Lai gan personām varētu nebūt iebildumu pret videonovērošanu drošības nolūkā, ir jānodrošina, ka personas dati netiek izmantoti ļaunprātīgi pilnīgi atšķirīgiem un datu subjektam negaidītiem mērķiem, piemēram, sejas atpazīšanai.

Ar likumīguma principu ir cieši saistīts nolūka ierobežojuma princips, kas ir paredzēts Hartas 8. panta 2. punktā, VDAR 5. (1) (b) pantā, Policijas direktīvas 4. panta 1. punkta b) apakšpunktā un Konvencijas 108+ 5. panta 4. punkta b. apakšpunktā. Tas paredz, ka personas dati tiek vākti konkrētos, skaidros un leģitīmos nolūkos un to turpmāku apstrādi neveic ar minētajiem nolūkiem nesavietojamā veidā. Datu apstrādes nolūks ir jānosaka no paša sākuma, kad dati tiek vākti, un datus turpmāk var apstrādāt noteiktajā nolūkā. Pirms jebkādas turpmākas apstrādes ir jāapsver, vai jaunās apstrādes mērķi ir saderīgi ar sākotnēji definētajiem mērķiem. Pretējā gadījumā jaunajai apstrādei būs nepieciešams noteikts tiesisks pamats.

Saskaņā ar VDAR 6. panta 4. punktu, lai apstrādātu datus citā nolūkā nekā tas, kādā personas dati tika vākti, ir jāsaņem datu subjekta piekrišana, vai arī to var veikt, pamatojoties uz ES vai dalībvalsts tiesību aktiem, kas demokrātiskā sabiedrībā ir vajadzīgs un samērīgs pasākums, lai aizsargātu 23. panta 1. punktā noteiktās svarīgās sabiedrības intereses, piemēram, valsts drošību un aizsardzību, sabiedrisko drošību, noziedzīgu nodarījumu novēršanu, izmeklēšanu un atklāšanu. Citos gadījumos pārzinim ir jāpārliecinās, vai apstrāde citā nolūkā ir savietojama ar nolūku, kādā personas dati sākotnēji tika vākti, cita starpā ņemot vērā

a) jebkuru saikni starp nolūkiem, kādos personas dati ir vākti, un paredzētās turpmākās apstrādes nolūku;
b) kontekstu, kādā personas dati ir vākti, jo īpaši saistībā ar datu subjektu un pārziņa attiecībām;
c) personas datu raksturu, jo īpaši – vai ir apstrādātas īpašas personas datu kategorijas un vai ir apstrādāti personas dati, kas attiecas uz sodāmību un pārkāpumiem;
d) paredzētās turpmākās apstrādes iespējamās sekas datu subjektiem;
e) atbilstošu garantiju esamību, kas var ietvert šifrēšanu vai pseidonimizāciju (VDAR 6. panta 4. punkts).

Policijas direktīvas 4. panta 2. punkts paredz, ka apstrāde, ko veic tas pats vai cits pārzinis, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināLsodus, bet ja šie nolūki nav tie paši, kādos personas dati tika vākti, ir atļauta, ciktāl:

a) pārzinim šādos nolūkos ir atļauts apstrādāt šādus personas datus saskaņā ar ES vai dalībvalsts tiesībām un
b) apstrāde ir vajadzīga un samērīga ar minētajiem citiem nolūkiem saskaņā ar ES vai dalībvalsts tiesībām.

Prasība, lai apstrāde citā nolūkā būtu savietojama ar to iepriekšējās apstrādes nolūku, ir būtiska attiecībā uz sejas atpazīšanas tehnoloģiju izmantošanu kā privātā, tā publiskā sektorā. Eiropas Padome atgādina – ja piekrišana tiek dota konkrētam mērķim, personas datus nevajadzētu apstrādāt veidā, kas nav saderīgs ar šo mērķi. Līdzīgi, ja datus atklāj trešajai personai, arī šādai izpaušanai vajadzētu saņemt īpašu piekrišanu.[560] Jautājums par datu apstrādes mērķa noteikšanu un savietojamību ir aktuāls arī attiecībā uz valsts iestādēm, kas apstrādā datus terorisma vai citu smagu noziedzīgu nodarījumu apkarošanai. Tas ir vispāratzīts nolūks, kas ļauj piekļūt ES un nacionālajām datubāzēm. Izstrādājot informācijas tehnoloģijas sistēmas, tostarp sejas atpazīšanas sistēmas, pastāv risks, ka personas datus (sejas attēlus) var izmantot mērķiem, kas sākotnēji nebija paredzēti, lai apmācītu vai veidotu sejas atpazīšanas tehnoloģijas, prettiesiski piekļūstot liela mēroga datubāzēm, t. i., mērķiem, kādiem šie dati iepriekš nebija paredzēti.[561]

Viens no pašlaik aktuāliem jautājumiem – vai un kādos gadījumos tiesībaizsardzības iestādes var iegūt un izmantot informāciju no sociālo mediju kontiem. Piemēram, tie tika plaši izmantoti, lai sameklētu protestētājus, kas 2021. gada janvārī ielauzās Kapitolija ēkā ASV Vašingtonā.[562] Lai gan VDAR un Policijas direktīva ļauj apstrādāt īpašas kategorijas personas datus, ja datu subjekts tos ir publiskojis (VDAR 9. panta 2. punkta e) apakšpunkts un Policijas direktīvas 10. pants), tomēr tas nenozīmē, ka sejas atpazīšanas tehnoloģijās ir atļauts integrēt personas publicētos sejas attēlus. Eiropas Padome 2021. gadā publicētajās Vadlīnijās par sejas atpazīšanu norāda, ka digitālo attēlu, kas ir augšupielādēti internetā, tostarp sociālajos tīklos vai tiešsaistes fotoattēlu pārvaldības vietnēs, vai kas uzņemti ar videonovērošanas kamerām, izmantošanu nevar uzskatīt par likumīgu tikai tāpēc, ka personas šos datus ir darījušas acīmredzami pieejamus. Likumdevējiem un lēmumu pieņēmējiem ir jānodrošina, ka digitālā formātā, piemēram,

560 Council of Europe (2021), .. Convention 108.

561 FRA (2019), Facial recognition technology.

562 Stone, M., Bartz, D. (8 January, 2021). Some U.S. Capitol rioters fired after internet detectives identify them. *Reuters.* https://www.reuters.com/article/us-usa-election-protests-fallout-idUSKBN29C36M

sociālajos tīklos, pieejamus attēlus nevar apstrādāt, lai iegūtu biometriskās veidnes vai integrētu tās biometriskās sistēmās bez konkrēta tiesiska pamata jaunai apstrādei, kad šie attēli sākotnēji tika uzņemti citiem mērķiem. Tā kā biometrisko veidņu iegūšana no digitālajiem attēliem ietver sensitīvu datu apstrādi, ir jānodrošina tiesiskais pamats, kas dažādās nozarēs un izmantošanas gadījumos atšķiras.[563]

6.2.2. Godprātība un pārredzamība

Tā kā novērošanas tehnoloģijas var izmantot bez jebkādas sadarbības ar datu subjektiem, apstrādes pārredzamība un godprātība (*fairness* – angļu val.) ir ļoti nozīmīgas. Godprātības princips ir vērsts uz godīgām attiecībām starp datu pārzini un datu subjektu un paredz, ka personas dati netiks iegūti negodīgā ceļā un par to neinformējot. Tas nozīmē, ka pārzinis ievēro VDAR noteiktos pienākumus, to skaitā informē datu subjektu par datu apstrādi, izvērtē personas datu apstrādes ietekmi uz datu subjektu un spēj pierādīt apstrādes darbību atbilstību VDAR. Šis princips arī paredz, ka pārzinim pēc iespējas ir jāuzklausa un jāņem vērā datu subjekta vēlmes par viņa datu apstrādi, it īpaši tad, ja datu apstrādes tiesiskais pamats ir piekrišana.[564] Godprātības princips ir cieši saistīts ar pārredzamības principu.

Pārredzamības principa mērķis ir radīt uzticību sistēmām un datu apstrādes procesiem un, ja nepieciešams, tos apstrīdēt.[565] Pārredzamība ir visaptverošs princips, kas attiecas uz trim galvenajām jomām. Tās ir:

1) informācijas sniegšana datu subjektiem saistībā ar godprātīgu apstrādi;
2) datu pārziņa saziņa ar datu subjektiem saistībā ar viņu tiesībām saskaņā ar VDAR; un
3) pārziņa darbība atvieglojot datu subjektiem viņu tiesību izmantošanu.[566]

Godprātīgas un pārredzamas apstrādes principi paredz, ka personas ir jāinformē par novērošanas tehnoloģiju izmantošanu un apstrādes nolūkiem. VDAR 60. apsvērums nosaka: "[..] datu subjekts ir jāinformē par apstrādes darbības esamību un tās nolūkiem." Datu subjekts jāinformē arī par profilēšanas esamību un šādas profilēšanas sekām.

Godprātības un pārredzamības princips rada daudz jaunu jautājumu par mākslīgo intelektu un lielajiem datiem, ņemot vērā sarežģīto datu apstrādi

563 Council of Europe (2021), .. Convention 108.

564 ES Pamattiesību aģentūra, ECT, EP, EDAU (2018), Rokasgrāmata, 118. lpp.

565 Article 29 Data Protection Working Party. (2017). Guidelines on transparency under Regulation 2016/679. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

566 Ibid.

mākslīgā intelekta sistēmās, iznākuma nenoteiktību un mērķu daudzveidību. No minētajiem principiem izriet prasība nodrošināt informāciju par automatizētas lēmumu pieņemšanas esamību un sniegt nozīmīgu informāciju par tā loģiku un paredzamajām sekām, t. i., nodrošināt automatizētu lēmumu izskaidrojamību. Iespējams, ka pārredzamības kā izskaidrojamības ideju var attiecināt arī uz automatizētiem secinājumiem, pat ja konkrēts lēmums vēl nav pieņemts. Pastāv neskaidrība par to, ko nozīmē automatizēta lēmuma loģika un sekas. Attiecībā uz sarežģītu mākslīgā intelekta apstrādi pastāv konflikts starp nepieciešamību sniegt īsu un viegli saprotamu informāciju, no vienas puses, un precīzu un padziļinātu informāciju, no otras puses.

Saistībā ar godprātības principu var runāt arī par automatizētu lēmumu satura godprātīgumu jeb taisnīgumu (*faireness* – angļu val.).[567] VDAR 71. apsvērums nosaka: "Lai nodrošinātu godprātīgu un pārredzamu apstrādi attiecībā uz datu subjektu, ņemot vērā konkrētos apstākļus un kontekstu, kurā personas dati tiek apstrādāti, pārzinim būtu jāizmanto piemērotas matemātiskās vai statistikas procedūras profilēšanai, jāveic atbilstīgi tehniski un organizatoriski pasākumi, lai it īpaši nodrošinātu, ka tiek koriģēti faktori, kuru dēļ rodas personas datu neprecizitātes, un ka līdz minimumam ir samazināts kļūdu rašanās risks, jāgarantē personas datu drošība tādā veidā, lai ņemtu vērā iespējamos riskus attiecībā uz datu subjekta interesēm un tiesībām un lai cita starpā novērstu fizisku personu diskrimināciju dēļ rases vai etniskās izcelsmes, politiskajiem uzskatiem, reliģiskās vai ticības piederības, dalības arodbiedrībā, ģenētiskā vai veselības stāvokļa vai dzimumorientācijas, vai izrietošus pasākumus, kas izraisa šādu diskrimināciju. Automatizēta lēmumu pieņemšana un profilēšana, pamatojoties uz īpašām personas datu kategorijām, būtu jāatļauj tikai saskaņā ar konkrētiem nosacījumiem."

Pārredzamība var paredzēt arī piekļuvi datiem, it īpaši mākslīgā intelekta sistēmu apmācāmajai datu kopai. Piekļuve datiem var būt nepieciešama, lai noteiktu iespējamos netaisnīguma cēloņus, kas izriet no nepietiekamiem vai neobjektīviem datiem vai apmācības algoritma. Tas ir īpaši svarīgi, ja algoritmiskais modelis ir necaurspīdīgs, kā rezultātā, to pārbaudot, nevar atklāt iespējamos trūkumus.[568]

Personas ir jāinformē par riskiem, noteikumiem, aizsardzības pasākumiem un tiesībām saistībā ar personas datu apstrādi un to, kā īstenot savas tiesības saistībā ar šādu apstrādi (VDAR 39. apsvērums). Personām ir jābūt informētām, ka viņu personas datus vāc, izmanto vai citādi apstrādā, un kādā apjomā tie tiek vai

567 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

568 Profilēšanas un automatizētu lēmumu pieņemšanas prasības vairāk apskatītas grāmatas 6.3. nodaļā.

tiks apstrādāti. Pārredzamības principa pamatā ir prasība, ka visa informācija un saziņa, kas saistīta ar personas datu apstrādi, tiek sniegta kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu (VDAR 12. panta 1. punkts, 39., 58. apsvērums). VDAR 12.–14. pants paredz, kādā veidā un kāda informācija ir jāsniedz datu subjektam. VDAR nosaka pārzinim pienākumu sniegt datu subjektam informāciju par personas datu apstrādi, ja dati tiek iegūti no datu subjekta (13. pants)[569], kā arī ja tie nav iegūti no datu subjekta (14. pants). Tomēr pārredzamības principu un informēšanas pienākumu var ierobežot saskaņā ar tiesību aktiem, lai garantētu tiesībaizsardzības mērķus, piemēram, sabiedrības drošību, ievērojot samērīguma principu saskaņā ar VDAR 23. pantu.

Policijas direktīva neparedz pārredzamības principu, un tas var šķist loģiski, jo vairākumā gadījumu sistemātiska pārredzamība kavē noziedzības novēršanas darbību vai valsts iestādes kriminālizmeklēšanas efektivitāti. Tajā pašā laikā Policijas direktīvā kā princips ir paredzēts godprātīga apstrāde (4. panta 1. punkta a) apakšpunkts), un tas var prasīt zināmu pārredzamību. Turklāt 23. apsvērums paredz, ka jebkurai personas datu apstrādei ir jābūt likumīgai, godprātīgai un pārredzamai attiecībā uz personām un jātiek īstenotai tikai konkrētos likumā paredzētos nolūkos. Tas pats par sevi neliedz tiesībaizsardzības iestādēm veikt tādas darbības kā slepena izmeklēšana vai videonovērošana. Šādas darbības var veikt, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu, ja vien šīs darbības ir paredzētas

569 Saskaņā ar VDAR 13. panta 1. punktu, ja pārzinis personas datus vāc no datu subjekta, tam personas datu iegūšanas laikā datu subjektam ir jāsniedz šāda informācija: pārziņa identitāte un kontaktinformācija; attiecīgā gadījumā – datu aizsardzības speciālista kontaktinformācija; apstrādes nolūki, kam paredzēti personas dati un apstrādes juridiskais pamats; pārziņa vai trešās personas leģitīmās intereses, ja apstrāde pamatojas uz šo juridisko pamatu; personas datu saņēmēji vai saņēmēju kategorijas; informācija par datu nosūtīšanu uz trešo valsti vai starptautisku organizāciju un vai tā notiek, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību vai pamatojoties uz atbilstošām garantijām.
VDAR 13. panta 2. punkts paredz, ka papildus minētajai informācijai pārzinis personas datu iegūšanas laikā datu subjektam sniedz arī papildu informāciju, kas vajadzīga, lai nodrošinātu godprātīgu un pārredzamu apstrādi. Šī informācija ir: laikposms, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto laikposma noteikšanai; datu subjekta tiesības saistībā ar apstrādi, piemēram, tiesības piekļūt datiem, ierobežot to apstrādi, dzēst datus, iebilst pret datu apstrādi; tiesības iesniegt sūdzību uzraudzības iestādei; informācija, vai personas datu sniegšana ir noteikta saskaņā ar likumu vai līgumu, vai tā ir priekšnosacījums, lai līgumu noslēgtu, kā arī vai datu subjektam ir pienākums personas datus sniegt un sekas datu nesniegšanas gadījumā; informācija par automatizēta lēmumu pieņemšanu, tai skaitā profilēšanu, un, ja šādi lēmumi rada tiesiskās sekas vai līdzīgā veidā ievērojami ietekmē datu subjektu, vai ietver īpašas personas datu kategorijas, informācija par tajos ietverto loģiku, kā arī apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu.

likumā un ir nepieciešamas un samērīgas demokrātiskā sabiedrībā, pienācīgi ņemot vērā attiecīgās fiziskās personas leģitīmās intereses.

Personas ir jāinformē par riskiem, noteikumiem, garantijām un tiesībām saistībā ar personas datu apstrādi un to, kā īstenot savas tiesības saistībā ar apstrādi. Policijas direktīvas 13. pants nosaka, kāda informācija ir jādara pieejama vai jāsniedz datu subjektam, un 14. pants nosaka datu subjekta piekļuves tiesības.

Konvencijas 108+ 5. panta 4. punkts paredz, ka personas dati ir jāapstrādā taisnīgi un pārredzami. Līdz ar jaunajiem grozījumiem Konvencija 108+ tika papildināta ar 8. pantu, kas nosaka datu apstrādes pārredzamības prasības. Saskaņā ar minētā panta pirmo daļu katra puse nodrošina, ka pārzinis informē datu subjektus par:

a) viņa identitāti un pastāvīgo dzīvesvietu vai uzņēmumu;
b) paredzētās apstrādes tiesisko pamatu un mērķi;
c) apstrādāto personas datu kategorijām;
d) personas datu saņēmējiem vai saņēmēju kategorijām, ja tādas ir; un
e) līdzekļiem, kā izmantot datu subjekta tiesības; kā arī visu nepieciešamo papildu informāciju, lai nodrošinātu personas datu taisnīgu un pārredzamu apstrādi.

Eiropas Padome norāda – ja reāllaika sejas atpazīšanas tehnoloģijas tiek izmantotas nekontrolētā vidē, tiesībaizsardzības iestādes var izmantot slāņveida pieeju, sniedzot nepieciešamo informāciju datu subjektiem, kuri atrodas konkrētajā vietā. Pirmajā informācijas sniegšanas slānī jāsniedz lasāma un saprotama informācija par apstrādes mērķi, iestādi, kas izmanto attiecīgo tehnoloģiju, apstrādes ilgumu un vietu, kurā šī tehnoloģija darbojas, un tā jāpiestiprina atbilstošā tuvumā vietai, kur tā tiek izmantota. Informācijas sniegšanas otrajā slānī jānorāda visa nepieciešamā informācija saskaņā ar Konvencijas 108+ 8. pantu, kas jāizliek pie ieejas vietā, kur tehnoloģija tiek izmantota.[570] Gadījumā, ja tiesībaizsardzības iestādes datubāzes izveidotas identifikācijas vai pārbaudes nolūkā, pārredzamības pienākumu var proporcionāli ierobežot, lai tas neskartu tiesībaizsardzības mērķus saskaņā ar Konvencijas 108+ 11. pantu un ievērojot tās prasības.

Eiropas Padome skaidro, ka faktori, kas nosaka, vai tiek nodrošināta pārredzamība, ietver, piemēram, informācijas sniegšanu personām, vākšanas kontekstu, pamatotas cerības par to, kā dati tiks izmantoti, vai informāciju, ka sejas atpazīšana ir tikai produkta vai pakalpojuma funkcija vai arī tā neatņemama sastāvdaļa. Būtu jāsniedz informācija arī par to, kā sejas atpazīšanas datu vākšana, izmantošana vai koplietošana varētu ietekmēt personas, it īpaši, ja šie dati attiecas uz personām, kuras atrodas neaizsargātās situācijās. Sniegtajai informācijai arī jānorāda, kādas datu subjektam ir tiesības un tiesiskās aizsardzības

570 Council of Europe (2021), .. Convention 108.

līdzekļi.[571] Pārredzamības princips ne tikai nosaka pienākumu informēt konkrētās personas par novērošanas tehnoloģiju izmantošanu un datu apstrādi, bet tas ir arī skatāms plašāk – kā pienākums informēt sabiedrību par šādu tehnoloģiju ieviešanu un izmantošanu, lai veicinātu sabiedrības izpratni un līdzdalību. Šis jautājums aplūkots grāmatas 7.7. nodaļā.

6.2.3. Datu minimizēšana

Datu minimizēšanas princips uzliek pienākumu noteikt minimālo personas datu apjomu, kas nepieciešams konkrētā mērķa sasniegšanai, un neapstrādāt vairāk informācijas, nekā tas ir nepieciešams šim mērķim. VDAR noteiktais datu minimizēšanas princips paredz, ka personas dati ir "adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams to apstrādes nolūkos" (5. panta 1. punkta c) apakšpunkts). Līdzīgi minētais princips ir noteikts Konvencijas 108+ 5. panta 4. punkta c) apakšpunktā. Policijas direktīva arī nosaka, ka dalībvalstis paredz, ka personas dati ir "atbilstīgi, būtiski un nav pārmērīgi, ņemot vērā nolūkus, kādos tos apstrādā" (4. panta 1. punkta c) apakšpunkts).

Mākslīgā intelekta sistēmām parasti ir nepieciešams liels datu apjoms. Dž. Sartors norāda, ka pastāv saspīlējums starp minimizēšanas principu un lielo datu un datu analīzes ideju, kas ietver mākslīgā intelekta un statistikas metožu izmantošanu, lai atklātu jaunas negaidītas korelācijas plašās datu kopās, tomēr šo pretrunu var mazināt. Datu aizsardzības pamatprincipi – īpaši nolūka ierobežošana un datu minimizēšana – jāinterpretē tā, lai tie neizslēgtu personas datu izmantošanu mašīnmācīšanās nolūkos. Tiem nevajadzētu izslēgt algoritmisko modeļu apmācīšanai paredzēto datu kopu (*training sets* – angļu val.) un algoritmisko modeļu izveidi, ja vien mākslīgā intelekta radītās sistēmas ir sociāli izdevīgas un atbilst datu aizsardzības tiesībām.[572]

Datu minimizēšanas princips paredz piemērot proporcionalitātes jeb samērīguma principu, lai iepriekš noteiktos leģitīmos nolūkus īstenotu ar minimāli nepieciešamo datu apjomu. Datu pārzinim ir jāizvērtē, vai konkrētie dati ir nepieciešami noteiktajam nolūkam un vai ir iespējams samazināt apstrādāto datu apjomu. Veidojot mašīnmācīšanās sistēmas, ir jāapsver, vai personas dati ir jāapstrādā konkrētajam mērķim un vai var sasniegt to pašu rezultātu, apstrādājot mazāk datu vai iekļaujot mazāk personu.[573]

571 Council of Europe (2021), .. Convention 108.

572 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

573 ICO (2023). Guidance on AI and data protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

Lai ievērotu minimizēšanas principu, dažos gadījumos ir iespējams samazināt pieejamo datu "personīgumu", nevis datu apjomu, lai datus nevarētu viegli savienot ar indivīdiem, piemēram, izmantojot pseidonimizāciju. Atkārtota identifikācija būtu stingri jāaizliedz, ja vien nav izpildīti visi personas datu tiesiskas vākšanas nosacījumi un ja vien tā ir saderīga ar mērķiem, kādiem dati sākotnēji tika vākti, un pēc tam dati tiek anonimizēti.[574]

Uz personas datu apstrādi dažkārt var attiekties brīvākas minimizēšanas prasības, piemēram, apstrādājot tos statistikai. Tomēr statistikas nolūkā veiktas datu apstrādes beigās nedrīkstētu būt konkrētu personu dati. Informācija, ko izmanto, lai personu pieskaitītu grupai, un ziņas par personas piederību šai grupai, ir personas dati, tātad arī secinātie dati par šo personu. Personas dati ir arī jebkura informācija par cilvēkiem, ko iegūst no datu kopām, lai pieņemtu lēmumus, kas viņus ietekmē, pamatojoties uz grupas profilēšanas informāciju.[575]

6.2.4. Precizitāte

Precizitātes princips uzliek pienākumu nodrošināt, ka "personas dati ir precīzi un, ja vajadzīgs, atjaunināti", kā arī veikt saprātīgus pasākumus, lai nodrošinātu, ka neprecīzi personas dati tiek dzēsti vai laboti (VDAR 5. panta 1. punkta d) apakšpunkts, Policijas direktīvas 4. panta 1. punkta d) apakšpunkts). Arī Konvencijas 108+ 5. panta 4. punkta d) apakšpunkts paredz, ka apstrādājamajiem personas datiem ir jābūt precīziem un, ja nepieciešams, tie regulāri jāatjaunina.

Šis princips attiecas arī uz personas datiem, kas tiek izmantoti, lai apmācītu mākslīgā intelekta algoritmus. Noteiktas grupas locekļus var skart aizspriedumi, ja šo grupu pārstāv tikai ļoti neliela apmācāmās datu kopas apakškopa, jo tas samazinās šīs grupas prognozes precizitāti. It īpaši liels risks ir gadījumā, ja personas dati tiek izmantoti secinājumu izdarīšanai vai lēmumu pieņemšanai par personu.

Vienas no lielākajām bažām attiecībā uz mākslīgā intelekta novērošanas tehnoloģiju izmantošanu ir, ka tās nav pietiekami precīzas. Kļūdaini rezultāti ir saistīti arī ar datu kvalitāti un datu apstrādes precizitāti. Lai nodrošinātu precīzu apstrādi, nepieciešama regulāra novērošanas sarakstā iekļauto sejas attēlu labošana un atjaunināšana. Attiecībā uz kļūdu līmeni jāpatur prātā – algoritms nekad nesniedz precīzu rezultātu, bet tikai varbūtības, piemēram, – 80 % varbūtība, ka novērošanas sarakstā vienā attēlā redzamā persona ir tā pati, kas redzama citā attēlā. Precizitātes novērtējums jāveic dažādām iedzīvotāju grupām, jo vispārējie precizitātes rādītāji var būt maldinoši. Piemēram, sejas atpazīšanas tehnoloģiju

574 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

575 Ibid.

precizitāte var būt atšķirīga atkarībā no personas dzimuma, vecuma un etniskās grupas.[576]

Eiropas Padome vērš uzmanību, ka iestādēm ir jānodrošina, lai biometriskās veidnes un digitālie attēli būtu precīzi un atjaunināti. Piemēram, ir jāpārbauda novērošanas sarakstos ievietoto attēlu un biometrisko veidņu kvalitāte, lai novērstu iespējamu nepatiesu atbilstību, jo zemas kvalitātes attēli var palielināt kļūdu skaitu. Tas ir tieši saistīts ar novērošanas sarakstā apkopoto attēlu avotiem, kas prasa stingri ievērot tādus datu aizsardzības principus kā nolūka ierobežošana. Nepatiesas atbilstības gadījumā iestādēm ir jāveic visi saprātīgie pasākumi, lai nodrošinātu gadījumu atbilstību un digitālo attēlu un biometrisko veidņu precizitāti.[577]

6.2.5. Glabāšanas ierobežojums

Glabāšanas ierobežojuma princips paredz, ka personas dati tiek glabāti veidā, kas pieļauj datu subjektu identifikāciju ne ilgāk, kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā (VDAR 5. panta 1. punkta e) apakšpunkts, Policijas direktīvas 4. panta 1. punkta e) apakšpunkts, Konvencijas 108+ 5. panta 4. punkta e) apakšpunkts). VDAR paredz izņēmumu, ka personas datus var glabāt ilgāk, ciktāl personas datus apstrādā tikai arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos, ar noteikumu, ka tiek īstenoti atbilstoši tehniski un organizatoriski pasākumi, lai aizsargātu datu subjekta tiesības un brīvības (5. panta 1. punkta e) apakšpunkts).

Lai nodrošinātu, ka personas dati netiek glabāti ilgāk, nekā nepieciešams, iestādei ir jānosaka termiņi, kad dati jādzēš, vai periodiski tie ir jāpārskata. Kad personas dati vairs nav nepieciešami noteiktajam nolūkam, tie ir jādzēš vai jāanonimizē.

Termiņš ir jānosaka arī sejas atpazīšanas sistēmās izmantoto biometrisko datu dzēšanai. Eiropas Padome norāda, ka, izmantojot sejas atpazīšanas tehnoloģijas reāllaikā, iestādēm jānodrošina, ka dažādiem apstrādes posmiem tiek piemēroti atšķirīgi glabāšanas periodi. Ja nav konstatēta atbilstība ar biometriskajām veidnēm, to personu datus, kuras iziet cauri nekontrolētai videi, nedrīkst glabāt, un dati ir automātiski jāizdzēš. Savukārt, ja ir konstatēta atbilstība, biometriskās veidnes drīkst glabāt stingri ierobežotu laiku, kā to nosaka tiesību akti, piemērojot nepieciešamos pasākumus. Arī atbilstības pārskatus, kas ietver personas datus, drīkst glabāt ierobežotu laiku. Jebkurā gadījumā novērošanas saraksts un

576 FRA (2019), Facial recognition technology.

577 Council of Europe (2021), .. Convention 108.

biometriskās veidnes ir jādzēš, beidzoties nolūkam, kam tika izmantotas sejas atpazīšanas tehnoloģijas.[578]

6.2.6. Datu drošība

Datu drošības princips ir noteikts VDAR 5. panta 1. punkta f) apakšpunktā (tas tiek saukts par "integritātes un konfidencialitātes principu") un Policijas direktīvas 4. panta 1. punkta f) apakšpunktā, kas paredz, ka personas dati tiek apstrādāti tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus. Līdzīgi datu drošības princips ir noteikts Konvencijas 108+ 7. panta 1. punktā.

Datu drošības princips tālāk konkretizēts VDAR 2. iedaļā (32.–34. pants), kā arī Policijas direktīvas 2. iedaļā (29.–30. pants). Pārzinim un apstrādātājam ir pienākums īstenot atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam. Pārzinim ir pašam jāizvērtē un jānosaka, kādi "atbilstoši pasākumi" ir īstenojami, ņemot vērā tehnikas līmeni (*the state of the art* – angļu val.), īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī riska iespējamību un smaguma pakāpi (VDAR 32. panta 1. punkts, Policijas direktīvas 29. panta 1. punkts). Uz risku balstīta pieeja uzliek pienākumu iestādei novērtēt apstrādei raksturīgos riskus un īstenot atbilstošus tehniskus un organizatoriskus pasākumus, kas būtu piemēroti, lai šos riskus mazinātu un novērstu, ievērojot, ka, jo augstāks ir risks, jo stingrāki ir pasākumi, kas jāveic (VDAR 83. apsvērums).

Datu drošība ir vēl jo svarīgāka, ja tiek apstrādāti biometriskie dati. Tā kā biometriskos datus apstrādā sejas atpazīšanas tehnoloģijas, tās rada ievērojamus drošības riskus, kurus ir grūti vai pat nav iespējams paredzēt. Biometriskos datus, kā pirkstu nospiedumus un sejas attēlus, nevar aizstāt. Ja tie tiek nozagti, tie ir zaudēti pavisam atšķirībā no citiem autentifikācijas veidiem, piemēram, no parolēm, kuras var nomainīt. Tādējādi jebkurš datu drošības pārkāpums var radīt īpaši smagas sekas datu subjektiem. Šādu sensitīvu datu neatļautu izpaušanu nevar labot. Lai aizsargātu sejas atpazīšanas datus un attēlu kopas pret datu pazaudēšanu un neatļautu piekļuvi vai izmantošanu visos apstrādes posmos, neatkarīgi no tā, vai tā ir vākšana, nosūtīšana vai glabāšana, būtu jāīsteno stingri drošības pasākumi gan tehniskā, gan organizatoriskā līmenī. Ir jāveic atbilstoši drošības pasākumi, lai novērstu konkrētajai tehnoloģijai raksturīgus uzbrukumus.

578 Council of Europe (2021), .. Convention 108.

VDAR 32. panta 1. punktā ir uzskaitīti vairāki pasākumi, kas cita starpā var tikt īstenoti:

a) personas datu pseidonimizācija un šifrēšana;
b) spēja nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību;
c) spēja laicīgi atjaunot personas datu pieejamību un piekļuvi gadījumā, ja ir noticis fizisks vai tehnisks negadījums;
d) process regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību.

Arī Policijas direktīva nosaka konkrētas prasības, kuras valstu tiesību aktos ir jāparedz kā pārziņa vai apstrādātāja pienākumi, kas īstenojami pēc risku izvērtēšanas, piemēram, piekļuves kontrole, datu nesēju kontrole, glabāšanas kontrole, lietotāju kontrole, datu piekļuves kontrole, komunikācijas kontrole, datu ievades kontrole, spēja atjaunot uzstādītās sistēmas ("atgūšana"), spēja nodrošināt, ka sistēma funkcionē tā, ka par tās darbības kļūdu parādīšanos tiek ziņots ("drošums") un ka saglabātie dati nevar tikt sabojāti sistēmas darbības traucējumu dēļ ("integritāte") (29. panta 2. punkts).

Par personas datu aizsardzības pārkāpumu pārzinim ir pienākums ziņot uzraudzības iestādei (VDAR 33. pants, Policijas direktīvas 30. pants), kā arī datu subjektam (VDAR 34. pants, Policijas direktīvas 31. pants). Konvencija 108+ arī paredz pienākumu pārzinim nekavējoties ziņot vismaz kompetentajai uzraudzības iestādei par datu pārkāpumiem, kas var nopietni traucēt datu subjektu tiesības un pamatbrīvības (7. panta 2. punkts).

Pārzinim ir jāziņo par pārkāpumu uzraudzības iestādei "bez nepamatotas kavēšanās, un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms" (VDAR 33. panta 1. punkts, Policijas direktīvas 30. panta 1. punkts). Izņēmums, kad pārzinis var neziņot par pārkāpumu uzraudzības iestādei, ir gadījumā, ja maz ticams, ka tas varētu radīt risku fizisku personu tiesībām un brīvībām.

Pārzinim ir pienākums ziņot par pārkāpumu arī datu subjektam, tomēr tikai gadījumā, ja pārkāpums varētu radīt augstu risku fizisku personu tiesībām un brīvībām (VDAR 34. panta 1. punkts, Policijas direktīvas 31. panta 1. punkts). Paziņojums datu subjektam nav jāsniedz, ja pārzinis izpildījis vienu no trim nosacījumiem:

1) ir īstenojis atbilstīgus tehniskus un organizatoriskus aizsardzības pasākumus, un šie pasākumi ir piemēroti personas datiem, ko skāris pārkāpums, jo īpaši tas attiecas uz tādiem pasākumiem, kas personas datus padara nesaprotamus personām, kurām nav pilnvaru piekļūt personas datiem, piemēram, šifrēšana;

2) ir veicis pasākumus, lai, visticamāk, vairs nepastāvētu risks attiecībā uz datu subjektu tiesībām un brīvībām;
3) ja tas pārzinim prasītu nesamērīgi lielas pūles; šādā gadījumā pārzinis var izmantot publisku saziņu vai līdzīgu pasākumu, ar ko datu subjekti tiek informēti vienlīdz efektīvā veidā (VDAR 34. panta 3. punkts, Policijas direktīvas 31. panta 3. punkts).

Eiropas Padome Sejas atpazīšanas vadlīnijās arī vērš uzmanību, ka par visiem datu drošības pārkāpumiem, kas var nopietni ietekmēt datu subjektu tiesības un pamatbrīvības, jāziņo uzraudzības iestādei un attiecīgā gadījumā datu subjektiem. Drošības pasākumiem vajadzētu attīstīties laika gaitā, reaģējot uz mainīgajiem draudiem un konstatētajām ievainojamībām. Tiem jābūt samērīgiem arī ar datu sensitivitāti, kontekstu, kurā tiek izmantota īpaša sejas atpazīšanas tehnoloģija, un ar datu izmantošanas mērķiem, kaitējuma iespējamību indivīdiem un citiem būtiskiem faktoriem. Stingra sejas atpazīšanas datu glabāšanas un iznīcināšanas prakse, izmantojot drošas procedūras un ievērojot pēc iespējas īsāku datu glabāšanas periodu, arī palīdz samazināt drošības draudus.[579]

Tiek veikti arvien jauni pētījumi par mākslīgā intelekta tehnoloģijām, meklējot veidus, kā aizsargāt biometrisko datu drošību. Nozares labā prakse var atvieglot drošības prasību ieviešanu, sniedzot norādes un ieteikumus, kā identificēt un novērtēt riskus un kādi pasākumi būtu ieviešami, lai mazinātu drošības riskus.[580]

6.2.7. Pārskatatbildība

Pārskatatbildības princips (*accountability* – angļu val.) paredz, ka pārzinis ir atbildīgs par visu iepriekš minēto datu aizsardzības pamatprincipu ievērošanu un "var to uzskatāmi pierādīt" (VDAR 5. panta 2. punkts, Policijas direktīvas 4. panta 4. punkts). Pārzinim ir jāvar uzskatāmi parādīt jeb pierādīt atbilstību visām datu aizsardzības prasībām, veicot "atbilstošus tehniskus un organizatoriskus pasākumus", ņemot vērā "apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisko personu tiesībām un brīvībām" (VDAR 24. panta 1. punkts, Policijas direktīvas 24. pants).

Pārskatatbildības princips uzliek pienākumu īstenot "atbilstošus tehniskus un organizatoriskus pasākumus", lai uzskatāmi parādītu, ka apstrādē tiek ievērotas visas datu aizsardzības prasības, kas paredzētas tam piemērojamā tiesiskajā

579 Council of Europe (2021), .. Convention 108.

580 Sk., piemēram, ICO. How should we assess security and data minimisation in AI? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/; ENISA. (2017). Handbook on Security of Personal Data Processing. https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

regulējumā. Pārzinis ir atbildīgs par datu apstrādes likumību, datu subjektu tiesību garantēšanu, datu drošības un citu prasību izpildi. Atbilstība var tikt demonstrēta, veicot dažādus pasākumus, tostarp: informējot datu subjektus par datu apstrādi (VDAR 13. pants); uzturot datu subjektu tiesību īstenošanas kārtību un procedūras, piemēram, piekļuves, labošanas un dzēšanas pieprasījumus (VDAR 12., 24. pants); īstenojot datu drošības pasākumus (VDAR 32. pants); uzturot personas datu apstrādes darbības reģistru (30. pants); veicot novērtējumu par ietekmi uz datu aizsardzību (VDAR 25. pants); nozīmējot datu aizsardzības speciālistu (VDAR 37. pants); noslēdzot personas datu apstrādes līgumu (VDAR 28. panta 3. punkts); sadarbojoties ar uzraudzības iestādi; pievienojoties rīcības kodeksam un sertificējot personas datu apstrādes darbības (VDAR 40., 42. pants); pieņemot vadlīnijas un procedūras; izglītojot un apmācot darbiniekus par datu aizsardzību; īstenojot pārbaudes procedūras (iekšējo un ārējo auditu).[581] Lai gan pārskatatbildības princips VDAR nav tieši attiecināts uz apstrādātāju, arī apstrādātājam ir pienākums pierādīt tam noteikto prasību izpildi, piemēram, vai ir noslēgts līgums ar datu pārzini (VDAR 28. panta 3. punkts).

Lai īstenotu pārskatatbildības principu, būtiska loma ir datu aizsardzības speciālista nozīmēšanai, kas ir obligāta prasība visām valsts iestādēm. Privātiem uzņēmumiem ir jāizvērtē, vai tiem ir pienākums to nozīmēt, kā arī to var darīt brīvprātīgi. Saskaņā ar Policijas direktīvas 32. pantu dalībvalstis paredz, ka pārzinis ieceļ datu aizsardzības speciālistu.

VDAR 37. panta 1. punkts nosaka pārziņiem un apstrādātājiem pienākumu iecelt datu aizsardzības speciālistu šādos trīs gadījumos:

1) apstrādi veic publiska iestāde vai struktūra;
2) pārziņa vai apstrādātāja pamatdarbība sastāv no apstrādes darbībām, kurām nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā;
3) pārziņa vai apstrādātāja pamatdarbības ietver īpašo kategoriju datu apstrādi vai personas datu par sodāmību un pārkāpumiem apstrādi plašā mērogā.

Ja tiek izmantotas tehnoloģijas, kas ietver biometrisko datu apstrādi, ir obligāti jāieceļ datu aizsardzības speciālists. VDAR nav definēts, ko nozīmē "plašs mērogs" un "regulāra un sistemātiska novērošana", bet to piemērošanu ir skaidrojusi 29. panta darba grupa.[582] Datu subjektu regulāra vai sistemātiska novērošana

581 Sk., piemēram, ICO, How should we assess security and data minimisation in AI?; ENISA (2017), Handbook on Security of Personal Data Processing.

582 Article 29 Data Protection Working Party. (2016). Guidelines on Data Protection Officers ('DPOs'). https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

ir, piemēram, profilēšana un vērtēšana, mērķorientētas reklāmas, atrašanās vietas izsekošana ar mobilās lietotnes starpniecību, fiziskās sagatavotības un veselības datu novērošana ar valkājamu ierīču starpniecību u. tml.

Datu aizsardzības speciālistu ieceļ, pamatojoties uz viņa profesionālo kvalifikāciju, jo īpaši speciālām zināšanām datu aizsardzības tiesību un prakses jomā un spēju pildīt speciālista uzdevumus (VDAR 37. panta 5. punkts). VDAR neizvirza konkrētākas profesionālās kvalifikācijas prasības.

FPDAL paredz, ka par datu aizsardzības speciālistu var iecelt personu, kura ir iekļauta Datu valsts inspekcijas datu aizsardzības speciālistu sarakstā vai cita persona (17. pants). Datu aizsardzības speciālistu sarakstā ir iekļauti speciālisti, kuri ir nokārtojuši DVI organizēto datu aizsardzības speciālistu kvalifikācijas eksāmenu (18.–19. pants). Tomēr pārzinim vai apstrādātājam ir iespēja iecelt par speciālistu arī citu personu, kas var apliecināt savu profesionālo kvalifikāciju citādā veidā.

Mākslīgā intelekta un citu informācijas sistēmu, produktu un pakalpojumu, kas balstās vai ietver personas datu apstrādi, izstrādei ir jābalstās uz integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principiem. Integrēta datu aizsardzība ietver dažādus atbilstošus tehniskus un organizatoriskus pasākumus, kurus pārzinis veic gan apstrādes līdzekļu noteikšanas, gan pašas apstrādes laikā, lai īstenotu datu aizsardzības principus un apstrādē integrētu vajadzīgās garantijas, lai ievērotu datu aizsardzības prasības un aizsargātu datu subjektu tiesības (VDAR 25. panta 1. punkts, Policijas direktīvas 20. pants). Lai nodrošinātu atbilstību minētajam principam, pārzinim ir jāizvērtē datu apstrādes darbību un sistēmu atbilstība datu aizsardzības prasībām un jāveic atbilstoši pasākumi, lai nodrošinātu datu aizsardzību un drošību. Šādi pasākumi var ietvert, piemēram, apstrādāto personas datu daudzuma samazināšanu, personas datu pseidonimizāciju, tiklīdz tas ir iespējams, pārredzamību attiecībā uz funkcijām un personas datu apstrādi, kas datu subjektam dod iespēju pārraudzīt datu apstrādi un pārzinim dod iespēju izveidot un uzlabot drošības pasākumus (VDAR 78. apsvērums).

Integrēta datu aizsardzība aptver visus sejas atpazīšanas tehnoloģiju datu apstrādes posmus. Uzņēmumiem, kas izmanto šīs tehnoloģijas identifikācijas vai verifikācijas nolūkos, ir jānodrošina, ka viņu izmantotie produkti vai pakalpojumi ir paredzēti biometrisko datu apstrādei saskaņā ar nolūka ierobežošanas, datu minimizēšanas un ierobežota uzglabāšanas ilguma principiem un jāintegrē visi pārējie nepieciešamie drošības pasākumi tehnoloģijās. Kad organizācijas nosaka šo tehnoloģiju tehniskās iezīmes, tām ir jāievieš šie principi savā projektā, lai nodrošinātu, ka to ieviešana atbilst tiesībām uz datu aizsardzību.[583]

583 Council of Europe (2021), .. Convention 108.

Princips datu aizsardzībai pēc noklusējuma paredz – pārzinis īsteno atbilstošus tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka pēc noklusējuma tiek apstrādāti tikai tādi personas dati, kas ir nepieciešami katram konkrētajam apstrādes nolūkam. Minētais pienākums attiecas uz vākto personas datu apjomu, to apstrādes pakāpi, glabāšanas laikposmu un to pieejamību. Īpaši svarīgi ir nodrošināt, ka pēc noklusējuma pārzinis personas datus bez personas līdzdalības nedara pieejamus nenoteiktam personu skaitam (VDAR 25. panta 2. punkts, Policijas direktīvas 20. panta 2. punkts).

Sistēmu izstrādātāji, programmatūras inženieri, informācijas drošības speciālisti un citas izstrādes procesā iesaistītās personas var izmantot uzraudzības iestāžu[584] un citu organizāciju, piemēram, ENISA[585], izdotās vadlīnijas par integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principu piemērošanu. Datu aizsardzības ekspertu iesaistīšana komandās, kas strādā pie tehnoloģijas izstrādes, kā arī datu aizsardzības prasību izvirzīšana tehniskajā specifikācijā palīdz nodrošināt datu aizsardzības pēc noklusējuma principa ievērošanu.[586]

Atbildības princips paredz, ka organizācijas īsteno atbilstīgu personas datu pārvaldības politiku, ciktāl tas ir samērīgi ar apstrādes darbībām. Minētie pasākumi ietver arī iekšējo procedūru (piemēram, personas datu aizsardzības politikas, informācijas sistēmu drošības politikas utt.) pieņemšanu un ieviešanu praksē, atbildīgo personu nozīmēšanu, regulāru apmācību veikšanu, lai ieviestu datu aizsardzības standartus organizācijas kultūrā. Pārzinim ir jāizstrādā un jāsaglabā dokumentācija, lai varētu gan datu subjektam, gan uzraudzības iestādei parādīt, kādus atbilstības pasākumus tas ir veicis.[587]

Konvencijas 108+ 10. pants nosaka, ka valstis nodrošina, ka pārziņi un attiecīgā gadījumā apstrādāji veic visus nepieciešamos pasākumus, lai izpildītu konvencijas saistības un lai saskaņā ar valstu tiesību aktiem varētu pierādīt, it īpaši uzraudzības iestādei, ka viņu veiktā datu apstrāde atbilst konvencijas noteikumiem.

Eiropas Padome norāda, ka, izmantojot sejas atpazīšanas tehnoloģijas, ir jāveic organizatoriski pasākumi. Tie ir:

584 Sk., piemēram, ICO. Data protection by design and by default. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

585 ENISA. (2016). Privacy Enhancing Technologies: Evolution and State of the Art, A Community Approach to PETs Maturity Assessment. https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art

586 FRA (2019), Facial recognition technology.

587 Sk. Article 29 Data Protection Working Party. (2010). Opinion 3/2010 on the principle of accountability. http://www.dataprotection.ro/servlet/ViewDocument?id=654

- pārredzamas politikas, procedūru un prakses īstenošana, lai nodrošinātu, ka sejas atpazīšanas tehnoloģiju pamatā ir datu subjektu tiesību aizsardzība;
- pārredzamības ziņojumu publicēšana par sejas atpazīšanas tehnoloģiju konkrētu izmantošanu;
- apmācības programmu un revīzijas procedūru izveidošana un nodrošināšana tiem, kas ir atbildīgi par sejas atpazīšanas datu apstrādi;
- iekšējās uzraudzības komitejas izveidošana, lai izvērtētu un apstiprinātu jebkādu apstrādi, kas saistīta ar sejas atpazīšanas datiem;
- piemērojamo prasību attiecināšana uz trešo personu pakalpojumu sniedzējiem, biznesa partneriem vai citām personām, kas izmanto sejas atpazīšanas tehnoloģiju (un piekļuves liegšana trešajām personām, kas tām neatbilst);
- publiskajā sektorā: iepriekšējas novērtēšanas ierobežojumu noteikšana publiskā iepirkuma procedūrās, iesaistot sejas atpazīšanas rīku piegādātājus, un minimālā darbības līmeņa novērtēšana attiecībā uz precizitāti, it īpaši attiecībā uz tiesībaizsardzības mērķiem.

Iestādēm un organizācijām, kas izmanto sejas atpazīšanas tehnoloģijas, ir jāveic nepieciešamie tehniskie pasākumi, lai nodrošinātu biometrisko datu kvalitāti, ievērojot starptautiski saskaņotus tehniskos standartus atkarībā no to izmantošanas konteksta. Tām ir jānodrošina, lai cilvēku pārraudzībai joprojām būtu izšķiroša nozīme, ja tiek veiktas darbības, kas balstās uz šo tehnoloģiju rezultātiem. Tas prasa ieviest organizatoriskos pasākumus, lai uzraudzītu, kā tiek pieņemti lēmumi, kas var būtiski ietekmēt indivīdus.[588]

6.3. Automatizēta lēmumu pieņemšana un cilvēka līdzdalības prasība

Mākslīgā intelekta sistēmas, kas balstās uz lielu datu apjomu, ļauj pieņemt automatizētus lēmumus, kas arvien plašāk tiek izmantoti arī publiskajā sektorā, to skaitā ir lēmumi, kas pieņemti, izmantojot novērošanas tehnoloģijas un prognozējošos algoritmus sabiedrības drošības un noziedzības apkarošanas interesēs. Grāmatā iepriekš jau minēts, ka sejas atpazīšanas tehnoloģiju algoritmi nekad nenodrošina pilnīgi precīzu rezultātu, bet gan tikai varbūtības. Lai gan šīs tehnoloģijas precizitāte arvien palielinās, vienmēr pastāv noteikts kļūdu līmenis, līdz ar to automatizētu rezultātu piemērošana var negatīvi ietekmēt personu, it

588 Council of Europe (2021), .. Convention 108.

īpaši, ja uz šo rezultātu pamata tiek pieņemts lēmums, kas rada personai negatīvas sekas.

Cilvēka virsvadība ir jauna prasība, kas ietverta MI akta priekšlikumā. Tā paredz, ka mākslīgā intelekta sistēmas lietošanas laikā fiziskai personai ir jāvar to efektīvi pārraudzīt, un tas nozīmē: spēju pilnībā izprast sistēmas iespējas un ierobežojumus; apzināties tendenci automātiski vai pārmēru paļauties uz mākslīgā intelekta sistēmas radītajiem iznākumiem (piemēram, sniedzot ieteikumu, kādu lēmumu pieņemt); spēju pareizi interpretēt augsta riska mākslīgā intelekta sistēmas radītos iznākumus; spēju izlemt nelietot mākslīgā intelekta sistēmu vai citādi neievērot sistēmas darbības iznākumu; spēju iejaukties sistēmas darbībā vai pārtraukt to katrā atsevišķā situācijā; spēju iejaukties augsta riska mākslīgā intelekta sistēmas darbībā vai pārtraukt to, izmantojot pogu "stop" vai līdzīgu procedūru (14. panta 4. punkts).[589] Turklāt attiecībā uz augsta riska sistēmām, ko paredzēts izmantot fizisku personu tālidentifikācijai reāllaikā un vēlāklaikā (III pielikuma 1. punkta a) apakšpunkts), jānodrošina, ka lietotājs turklāt neveic nekādas darbības vai nepieņem nekādu lēmumu, pamatojoties uz identifikāciju, kas izriet no attiecīgās sistēmas, ja to nav pārbaudījušas un apstiprinājušas vismaz divas fiziskas personas (MI akta priekšlikuma 14. panta 5. punkts). Cilvēka virsvadības prasība paredz cilvēka līdzdalību automatizētu lēmumu pieņemšanas gadījumā.

Lēmuma pieņemšana ir pilnībā automatizēta, kad tā notiek bez cilvēka līdzdalības. Automatizētu lēmumu pieņemšana var daļēji pārklāties vai notikt profilēšanas rezultātā, un to var veikt gan ar, gan bez profilēšanas. Arī profilēšana var notikt bez automatizētu lēmumu pieņemšanas.[590]

Profilēšana ir jebkura veida automatizēta personas datu apstrāde, kas izpaužas kā personas datu izmantošana nolūkā izvērtēt konkrētus ar fizisku personu saistītus personiskus aspektus, jo īpaši – analizēt vai prognozēt aspektus saistībā ar minētās fiziskās personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos (VDAR 4. panta 4. punkts).

Pastāv trīs iespējamie veidi, kā var izmantot profilēšanu. To var izmantot:

1) vispārīgai profilēšanai bez automatizētu lēmumu pieņemšanas;
2) lēmumu pieņemšanai, pamatojoties uz profilēšanu;
3) tikai automatizēta lēmumu pieņemšanai, tostarp profilēšanai, kas rada tiesiskas sekas vai līdzīgā veidā ievērojami ietekmē datu subjektu.[591]

589 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

590 Article 29 Data Protection Working Party. (2017, as last revised and adopted 2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/612053

591 Ibid.

Datu subjektam ir tiesības nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde, tostarp profilēšana, kas attiecībā uz datu subjektu rada tiesiskās sekas vai kas līdzīgā veidā ievērojami ietekmē datu subjektu (VDAR 22. panta 1. punkts, Policijas direktīvas 11. panta 1. punkts). Tomēr no šī aizlieguma ir pieļaujami izņēmumi. Saskaņā ar VDAR 21. panta 2. punktu izņēmuma kārtā šāds lēmums var tikt pieņemts, ja tas

1) ir vajadzīgs, lai noslēgtu vai izpildītu līgumu starp datu subjektu un datu pārzini;
2) pamatojas uz datu subjekta nepārprotamu piekrišanu; vai
3) ir atļauts saskaņā ar ES vai dalībvalsts tiesību aktiem, kuri ir piemērojami pārzinim un kuros ir arī noteikti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības, un leģitīmās intereses.

Pirmajos divos gadījumos datu pārzinim jāveic atbilstīgi pasākumi, lai aizsargātu datu subjekta tiesības un brīvības, un leģitīmās intereses – vismaz tiesības panākt cilvēka līdzdalību no pārziņa puses –, lai datu subjekts varētu paust savu viedokli un apstrīdēt lēmumu. Tomēr minētie lēmumi nevar tikt pamatoti ar īpašām personas datu kategorijām, izņemot, ja datu subjekts ir devis nepārprotamu piekrišanu vai apstrāde ir vajadzīga būtisku sabiedrības interešu dēļ, pamatojoties uz ES vai dalībvalsts tiesību aktiem, un tiek nodrošināti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības, un leģitīmās intereses (VDAR 21. panta 3. punkts).

Policijas direktīvas 11. panta 1. punkts nosaka – dalībvalstis paredz, ka lēmums, kas balstās tikai uz automātisku apstrādi, tostarp uz profilēšanu, un kas rada nelabvēlīgas juridiskas sekas attiecībā uz datu subjektu vai būtiski viņu ietekmē, ir aizliegts, ja vien tas nav atļauts ES vai dalībvalsts tiesībās, kurās ir paredzētas atbilstošas garantijas attiecībā uz datu subjekta tiesībām un brīvībām, vismaz attiecībā uz tiesībām panākt cilvēka iejaukšanos no pārziņa puses. Līdzīgi kā VDAR, Policijas direktīva arī paredz, ka automatizētus individuālus lēmumus nepamato ar īpašām personas datu kategorijām, tostarp biometriskajiem datiem, izņemot, ja tiek nodrošināti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības, un leģitīmās intereses (Policijas direktīvas 11. panta 2. punkts). Turklāt šī direktīva paredz būtisku nosacījumu, ka profilēšana, kas izraisa diskrimināciju pret fiziskām personām, pamatojoties uz īpašu kategoriju personas datiem, ir aizliegta saskaņā ar ES tiesībām (Policijas direktīvas 11. panta 3. punkts).

Aizsardzības pasākumi automatizētu lēmumu pieņemšanas gadījumā, it sevišķi tad, ja tiek apstrādāti biometriskie dati, ir šādi: tiesības apstrīdēt lēmumu; tiesības panākt cilvēka līdzdalību; tiesības būt informētam par to, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana; tiesības saņemt jēgpilnu informāciju par automatizētajā lēmumā ietverto loģiku, kā arī šādas apstrādes

nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu (VDAR 13. panta 2. punkta f) apakšpunkts, 14. a 2. punkta f) apakšpunkts).

Minētās normas paredz informēšanas pienākumu, un tās ir bijušas plašu diskusiju centrā, kur šī juridiskā prasība ir bijusi saistīta ar vispārīgāku un fundamentālu jautājumu par mākslīgā intelekta sistēmu un to rezultātu, kā arī ar to saistīto cilvēka pieņemto lēmumu izskaidrojamību (*explainability* – angļu val.).[592] Mākslīgā intelekta sistēmas un to lēmumi ir jāizskaidro. Cilvēkiem arī jāapzinās, ka viņi mijiedarbojas ar mākslīgā intelekta sistēmu. Pārredzamības prasība paredz, ka ir jāinformē par mākslīgā intelekta sistēmu iespējām un mērķiem, kā arī ierobežojumiem. Cilvēkiem ir jāsaprot, kā tiek izstrādātas, apmācītas un izmantotas mākslīgā intelekta sistēmas. Izskaidrojamība attiecas uz spēju izskaidrot gan sistēmas tehniskos procesus, gan ar tiem saistītos pieņemtos lēmumus. Tehniskā izskaidrojamība prasa, lai mākslīgā intelekta sistēmas pieņemtos lēmumus varētu saprast cilvēki. Pārredzamības prasības var atklāt, kā šīs sistēmas tiek izmantotas, lai veiktu prognozes, sniegtu ieteikumus vai pieņemtu lēmumus. Tās var atklāt kritērijus, kas ietekmē konkrētu prognozi vai lēmumu. Parasti šī prasība neparedz noteikta koda vai datu koplietošanu, jo tādējādi varētu tikt atklāts komercnoslēpums vai sensitīvi lietotāja dati. Tomēr daudzos gadījumos mākslīgā intelekta sistēmas ir pārāk sarežģītas, lai tās varētu izskaidrot. Ne vienmēr ir iespējams izskaidrot, kāpēc mākslīgā intelekta sistēma ir pieņēmusi konkrētu rezultātu vai lēmumu un kāda ievades faktoru kombinācija to veicināja. Šos gadījumus dēvē par "melno kasti" (*black box* – angļu val.), un to vietā varētu izmantot citus izskaidrojamības pasākumus, piemēram, izsekojamību, auditējamību un pārredzamu informāciju par sistēmas iespējām.

Līdzās informēšanai vēl viena būtiska garantija ir tiesības apstrīdēt automatizētus lēmumus. Atšķirībā no VDAR 22. panta 3. punkta Policijas direktīvā nav tieši noteiktas tiesības apstrīdēt automatizētus lēmumus, bet šīs tiesības ir pieminētas 38. apsvērumā, kur norādīts, ka katrā ziņā uz šādu apstrādi būtu jāattiecina atbilstošas garantijas, tostarp īpašas informācijas sniegšana datu subjektam un tiesības panākt cilvēka iejaukšanos, jo īpaši – paust savu viedokli, saņemt paskaidrojumu par lēmumu, kas pieņemts pēc šādas izvērtēšanas, un apstrīdēt lēmumu.

Konvencija 108+ arī nosaka personas tiesības nebūt tāda lēmuma subjektam, kas viņu būtiski ietekmē un kas pamatojas tikai uz automatizētu datu apstrādi, neņemot vērā viņa viedokli. Izņēmums, ja šāds lēmums ir atļauts ar tiesību aktu, kurā noteikti arī piemēroti pasākumi, lai aizsargātu datu subjekta tiesības,

592 Sk., piemēram, Barredo Arrieta, et al. (2020), Explainable Artificial Intelligence ..; Hamon, R., Junklewitz, H. and Sanchez, M. J. (2020). Robustness and Explainability of Artificial Intelligence. Publications Office of the European Union, Luxembourg. http://dx.doi.org/10.2760/57493; Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

brīvības un likumīgās intereses (9. panta 1. punkta a) apakšpunkts, 9. panta 2. punkts).

Eiropas Padome skaidro – ja sejas atpazīšanas tehnoloģiju izmantošana ir paredzēta, lai lēmumu varētu pieņemt, tikai un vienīgi pamatojoties uz automatizētu apstrādi, kas būtiski ietekmētu datu subjektu, datu subjektam it īpaši jābūt tiesībām, lai šāda apstrāde netiktu veikta bez viņa viedokļa uzklausīšanas. Ja, izmantojot reāllaika sejas atpazīšanas tehnoloģijas, personas vadās tikai pēc šo tehnoloģiju rezultātiem, to var uzskatīt par tikai automatizētu lēmumu pieņemšanu, kas iespējamās viltus sakritības dēļ var būtiski ietekmēt datu subjektu. Datu subjekts var pieprasīt, lai tiktu ņemts vērā viņa viedoklis.[593]

Svarīga prasība attiecībā uz tādu tehnoloģiju kā sejas atpazīšana izmantošanu ir tā, ka ikvienā gadījumā ir jānodrošina cilvēka iejaukšanās. Tas nozīmē, ka sakritības, kas tiek konstatētas ar šo tehnoloģiju, ir jāizvērtē, piemēram, policistam, kurš pārbaudīs šo sakritību un atbilstoši rīkosies. Šajā posmā jau tiek izslēgti daudzi viltus pozitīvi rezultāti.[594]

Jēdziens "automatizēta lēmumu pieņemšana" nav līdz galam skaidrs. Dažos gadījumos cilvēka iejaukšanās var būt vienkārši visu sistēmas rezultātu apstiprināšana, un tādējādi šis lēmums būs faktiski automatizēts. Būtu jāvērtē arī pretējie gadījumi, kad cilvēki pārskata un potenciāli atceļ sistēmas rezultātus. Pētījumi liecina, ka cilvēki atceļ algoritmu rezultātus galvenokārt tad, ja rezultāts atbilst viņu stereotipiem, un tā rezultātā, piemēram, mazākumtautību grupas var tikt nostādītas neizdevīgā stāvoklī. Šāda rīcība apdraud automatizētās apstrādes iespējamo pievienoto vērtību, jo tā var būt precīzāka vai atsevišķos gadījumos pat taisnīgāka.[595]

Vēl viena prasība, kas nav tieši noteikta VDAR, Policijas direktīvā un Konvencijā 108+, ir, ka lēmumam ir jābūt "saprātīgam" (*reasonable* – angļu val.). Tas nozīmē, ka lēmuma pieņemšanas mērķi ir atbalstāmi un izmantotās metodes ir uzticamas.[596]

6.4. Datu subjekta tiesības

ES datu aizsardzības regulējums datu subjektam paredz plaša apjoma tiesības:

- tiesības uz informāciju (VDAR 13., 14. pants, Policijas direktīvas 13. pants);
- piekļuves tiesības (VDAR 15. pants, Policijas direktīvas 14., 15. pants);

593 Council of Europe (2021), .. Convention 108.

594 FRA (2019), Facial recognition technology.

595 Ibid.

596 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

- tiesības labot datus (VDAR 16. pants, Policijas direktīvas 16. panta 1. punkts);
- tiesības dzēst datus (VDAR 17. pants, Policijas direktīvas 16. panta 2. punkts);
- tiesības ierobežot apstrādi (VDAR 18. pants, Policijas direktīvas 16. panta 3. punkts);
- tiesības uz datu pārnesamību (VDAR 20. pants);
- tiesības iebilst pret datu apstrādi (VDAR 21. pants);
- tiesības nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde, tostarp profilēšana (VDAR 22. pants, Policijas direktīvas 21. pants).

Līdzīgas tiesības datu subjektam paredz arī Konvencijas 108+ 9. pants:

a) tiesības nebūt automatizēta lēmuma subjektam;
b) tiesības saņemt apstiprinājumu par datu apstrādi, kas attiecas uz šo personu, saņemt informāciju saprotamā formā par apstrādātajiem datiem, to izcelsmi, saglabāšanas periodu, kā arī jebkuru citu informāciju, kas pārzinim jāsniedz, lai nodrošinātu datu apstrādes pārredzamību;
c) tiesības saņemt informāciju par datu apstrādes pamatojumu (*reasoning* – angļu val.), ja attiecībā uz personu tiek piemēroti šādas apstrādes rezultāti;
d) tiesības iebilst pret personas datu apstrādi, ja vien pārzinis nepierāda, ka tā tiesiskais pamatojums apstrādāt datus ir svarīgāks par personas interesēm vai tiesībām un pamatbrīvībām;
e) tiesības labot vai dzēst datus, ja tie tiek apstrādāti pretrunā ar konvencijas noteikumiem;
f) tiesības saņemt tiesiskās aizsardzības līdzekļus, ja ir pārkāptas personas tiesības saskaņā ar minēto konvenciju;
g) tiesības lūgt uzraudzības iestādes palīdzību, izmantojot savas tiesības.

Tā kā sejas atpazīšanas un citu mākslīgā intelekta novērošanas sistēmu pamatā ir personas datu apstrāde, datu subjektiem ir jāgarantē visas iepriekš uzskaitītās tiesības. Īpaša nozīme ir tiesībām uz informāciju, kas ir pārredzamības principa pamatā, un tiesībām nebūt automatizētu lēmumu subjektam. Būtiska nozīme mākslīgā intelekta tehnoloģiju izmantošanā ir arī pārējām tiesībām – piekļuves tiesībām, tiesībām iebilst, labot un dzēst datus, kā arī tiesībām uz efektīvu tiesību aizsardzību.

VDAR nosaka vispārīgas prasības attiecībā uz pārredzamas informācijas sniegšanu, saziņu un datu subjekta tiesību īstenošanas kārtību (VDAR 39. apsvērums, 12. pants, Policijas direktīvas 12. pants). Informācija ir jāsniedz kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu. Tā ir jāsniedz rakstiski, vajadzības gadījumā – elektroniskā formā, kā arī pēc datu subjekta pieprasījuma, un, ja ir pierādīta datu subjekta identitāte, to var sniegt arī mutiski (VDAR 12. panta 1. punkts, Policijas direktīvas 12. panta

1. punkts). Kad personas datus apstrādā, izmantojot elektroniskus līdzekļus, pārzinim ir jānodrošina arī līdzekļi, ar kuriem pieprasījumus var izdarīt elektroniski (VDAR 59. apsvērums un 12. panta 1. punkts, Policijas direktīvas 12. panta 1. punkts). Pārzinim ir jāatbild uz datu subjekta pieprasījumiem, kas saistīti ar šīs personas tiesību izmantošanu, un jāinformē par veiktajām darbībām bez nepamatotas kavēšanās (VDAR 12. panta 3. punkts, Policijas direktīvas 12. panta 3. punkts). VDAR nosaka, ka atbilde uz pieprasījumu ir jāsniedz mēneša laikā. Informācija ir jāsniedz bez maksas. Izņēmuma gadījumā, ja datu subjekta pieprasījumi ir acīmredzami nepamatoti vai pārmērīgi, it īpaši to regulāras atkārtošanās dēļ, pārzinis var vai nu pieprasīt saprātīgu maksu, vai arī atteikties izpildīt pieprasījumu. Tomēr šādā gadījumā pārzinim ir pienākums uzskatāmi parādīt, ka pieprasījums ir acīmredzami nepamatots vai pārmērīgs (VDAR 12. panta 5. punkts, Policijas direktīvas 12. panta 4. punkts). Pārzinim ir jāpārbauda datu subjekta, kas izdara pieprasījumu, identitāte, jo īpaši saistībā ar tiešsaistes pakalpojumiem un tiešsaistes identifikatoriem (VDAR 64. apsvērums, 12. panta 6. punkts, Policijas direktīvas 12. panta 5. punkts).

Datu subjektam ir tiesības piekļūt saviem datiem, lai iegūtu informāciju par apstrādi un pārliecinātos par tās likumīgumu. Piekļuves tiesības ietver tiesības saņemt apstiprinājumu par savu datu apstrādi, piekļūt attiecīgajiem datiem (t. i., iegūt to kopijas), kā arī iegūt detalizētu informāciju par apstrādi, tostarp apstrādes nolūku, personas datu kategorijām, personas datu saņēmējiem, laikposmu, cik ilgi personas dati tiks glabāti, informāciju par automatizētu lēmumu pieņemšanu u. c. (VDAR 15. panta 1. un 2. punkts, Policijas direktīvas 14. pants). Persona var pieprasīt par saviem datiem līdzīga veida informāciju, kas saskaņā ar VDAR pārzinim ir jāsniedz pirms personas datu apstrādes (VDAR 13. un 14. pants). Ja pārzinis apstrādā lielu informācijas apjomu saistībā ar datu subjektu, pārzinis var pieprasīt, lai datu subjekts jau laikus – pirms informācijas nosūtīšanas – precizē, uz kuru informāciju un kurām apstrādes darbībām pieprasījums attiecas (VDAR 15. panta 3. punkts). Pastāv neskaidrības, vai pārzinim ir jāsniedz datu subjektam tikai vispārīga informācija vai arī individuāls paskaidrojums.

Iespēja izmantot piekļuves tiesības ir daļa no tiesībām uz efektīvu tiesību aizsardzību. Lai gan datu subjekta tiesības uz piekļuvi nav tas pats, kas tiesības piekļūt lietas materiāliem, abas tiesības izriet no labas pārvaldības prasības. FRA norāda, ka tiesības uz labu pārvaldību ietver, bet neaprobežojas ar personas tiesībām piekļūt lietas materiāliem un jebkuras valsts iestādes pienākumu pamatot savus lēmumus. Piekļuve lietas materiāliem atvieglo izpratni par lēmuma pamatā esošiem pierādījumiem un iemesliem, tādējādi indivīdam dodot labākas iespējas izvirzīt pretargumentus, izmantojot tiesības tikt uzklausītam. Pienākums sniegt pamatojumu, raugoties no aizskarto personu pozīcijām, padara lēmumu pieņemšanas procesu pārredzamāku, lai attiecīgā persona varētu zināt, kāpēc ir veikts

pasākums vai darbība. Tiesības uz labu pārvaldību attiecas arī uz gadījumiem, kad tiesībaizsardzības iestādes apstrādā sejas attēlus, izmantojot sejas atpazīšanas tehnoloģijas.

Lai arī tiesības uz labu pārvaldību var būt pakļautas noteiktiem ierobežojumiem, rodas jautājums, kā nodrošināt, lai potenciāli milzīgajam personu skaitam būtu visa pieeja viņu failiem jeb glabātajiem personas datiem. Vēl viens jautājums ir, kā pārliecināties, ka policija un citas valsts iestādes vienmēr norāda iemeslus, ja kāds tiek apturēts un/vai meklēts, pamatojoties uz sejas atpazīšanas sakritību. Lai izmantotu tiesības piekļūt failiem, tostarp sistēmās saglabātajiem personas datiem, personai ir jāapzinās, ka tur tiek glabāti viņa personas dati. Cilvēki bieži nezina, ka viņu sejas attēli tiek ierakstīti un apstrādāti datubāzē salīdzināšanai. Ja viņi nezina par apstrādi, viņi arī nevar pieprasīt piekļuvi saviem datiem, kā arī izmantot citas tiesības. Tiesību uz labu pārvaldību galvenie komponenti, piemēram, tiesības piekļūt lietas materiāliem un iestādes pienākums pamatot savus lēmumus, ir skaidroti arī konkrētākos ES datu aizsardzības tiesību aktu noteikumos. Gan VDAR, gan Hartas 8. panta 2. punkts paredz, ka ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos.[597]

Datu subjektam ir arī tiesības uz savu personas datu labošanu, lai nodrošinātu, ka dati ir precīzi. Pēc datu subjekta pieprasījuma pārzinim ir pienākums bez nepamatotas kavēšanās labot neprecīzus šīs personas datus (VDAR 16. pants, Policijas direktīvas 16. panta 1. punkts). Iepriekš aplūkotais precizitātes princips uzliek pienākumu pašam pārzinim nodrošināt datu precizitāti, piemēram, regulāri lūdzot datu subjektam pārbaudīt savus personas datus. Neatbildēts paliek jautājums, kā nodrošināt to sejas attēlu precizitāti un atjaunošanu, kas izmantoti mākslīgā intelekta sistēmās. Viltus sakritības gadījumā datu subjekti var pieprasīt labojumus, lai izvairītos, ka sistēma nākotnē atkārtoti konstatē nepatiesu atbilstību.

Tiesības uz datu dzēšanu jeb tiesības "tikt aizmirstam" paredz datu subjekta tiesības panākt, lai pārzinis bez nepamatotas kavēšanās dzēstu datu subjekta personas datus, un pārziņa pienākums ir dzēst personas datus, ja vairs nepastāv personas datu likumīgas apstrādes nosacījumi (nosacījumi paredzēti VDAR 17. panta 1. punktā). Policijas direktīvas 16. panta 2. punkts nosaka, ka valstīm ir jāparedz, ka pārzinis bez nepamatotas kavēšanās dzēš personas datus un nodrošina datu subjektam tiesības panākt, lai pārzinis bez nepamatotas kavēšanās dzēstu personas datus, kas uz šo personu attiecas, ja apstrāde pārkāpj personas datu apstrādes pamatprincipus (4. pants), apstrādes likumības prasību (8. pants) vai īpašu kategoriju personas datu apstrādes nosacījumus (10. pants) vai ja personas dati ir jādzēš, lai izpildītu uz pārzini attiecināmu juridisku pienākumu.

597 FRA (2019), Facial recognition technology.

Neskaidrs ir jautājums, vai pienākums dzēst personas datus ietver arī izsecinātos personas datus vai arī izsecinātos grupas datus, piemēram, apmācīto algoritmisko modeli. Dž. Sartors uzskata, ka pirmajā gadījumā atbilde varētu būt pozitīva, bet otrajā negatīva, jo apmācītais algoritma modelis vairs nav personisks. Tajā pašā laikā, izdzēšot datus, ko izmanto algoritmiskā modeļa izveidošanai, var būt grūti vai neiespējami pierādīt šī modeļa pareizību.[598]

Policijas direktīvas 16. panta 3. punkts paredz, ka dzēšanas vietā pārzinis ierobežo apstrādi, ja

1) datu subjekts apstrīd personas datu precizitāti un to precizitāti vai neprecizitāti nevar noteikt;
2) personas dati ir jāsaglabā pierādījumu nolūkā.

Otrajā gadījumā pārzinis informē datu subjektu pirms apstrādes ierobežojuma atcelšanas.

Arī VDAR 18. panta 1. punkts nosaka, ka datu subjektam ir tiesības panākt, lai pārzinis ierobežotu apstrādi, ja ir viens no šādiem apstākļiem:

a) datu subjekts apstrīd personas datu precizitāti – uz laiku, kurā pārzinis var pārbaudīt personas datu precizitāti;
b) apstrāde ir nelikumīga, un datu subjekts iebilst pret personas datu dzēšanu un tās vietā pieprasa datu izmantošanas ierobežošanu;
c) pārzinim personas dati apstrādei vairs nav vajadzīgi, taču tie ir nepieciešami datu subjektam, lai celtu, īstenotu vai aizstāvētu likumīgas prasības;
d) datu subjekts ir iebildis pret apstrādi, līdz nav pārbaudīts, vai pārziņa leģitīmie iemesli nav svarīgāki par datu subjekta leģitīmajiem iemesliem.

Ja apstrāde ir ierobežota, personas datus ir atļauts tikai glabāt, bet apstrādāt tos citādā veidā var tikai ar datu subjekta piekrišanu vai tādēļ, lai celtu, īstenotu vai aizstāvētu likumīgas prasības, vai lai aizsargātu citas fiziskas vai juridiskas personas tiesības, vai ES vai dalībvalstu svarīgu sabiedrības interešu dēļ (VDAR 18. panta 2. punkts).

Policijas direktīva paredz datu subjektu tiesību ierobežojumus – piekļuves tiesību (15. pants), tiesību uz informāciju (13. panta 3. punkts), tiesību labot un dzēst datus un ierobežot datu apstrādi (16. panta 4. punkts) –, kas izriet no tiesībaizsardzības iestāžu pienākuma strādāt noteiktā konfidencialitātes un slepenības pakāpē un nodrošināt to darba efektivitāti. Ja datu apstrādes mērķis ir noziedzīgu nodarījumu novēršana, izmeklēšana, atklāšana vai kriminālvajāšana, kriminālsodu izpilde vai sabiedrības drošības nodrošināšana, minētās tiesības var tikt ierobežotas, ja tas nepieciešams, lai:

a) novērstu, ka tiek traucētas oficiālas vai juridiskas pārbaudes, izmeklēšanas vai procedūras;

598 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

b) novērstu, ka tiek kaitēts noziedzīgu nodarījumu novēršanai, atklāšanai, izmeklēšanai vai saukšanai pie atbildības par tiem, vai kriminālsodu izpildei;
c) aizsargātu sabiedrisko drošību;
d) aizsargātu valsts drošību;
e) aizsargātu citu personu tiesības un brīvības (Policijas direktīvas 13. panta 3. punkts, 15. panta 1. punkts, 16. panta 4. punkts).

Šiem ierobežojumiem ir jābūt noteiktiem tiesību aktos un ir jābūt nepieciešamiem un samērīgiem demokrātiskā sabiedrībā. Nacionālajā regulējumā ir jānosaka pārziņa pienākums bez nepamatotas kavēšanās rakstiski informēt datu subjektu par atteikumu vai ierobežojumu piekļūt datiem un par atteikuma vai ierobežojuma iemesliem, izņemot, ja tas apdraud kādu no minētajiem mērķiem. Pārzinim ir jāinformē datu subjekts arī par iespēju iesniegt sūdzību uzraudzības iestādei vai vērsties tiesā (Policijas direktīvas 15. panta 3. punkts). Pārzinim ir jādokumentē faktiskie vai juridiskie iemesli, kuri ir lēmuma pamatā, un šī informācija jādara pieejama uzraudzības iestādēm (Policijas direktīvas 15. panta 4. punkts). Pārzinim ir rakstiski jāinformē datu subjekts par atteikumu labot personas datus, tos dzēst vai ierobežot apstrādi un par atteikuma iemesliem.

VDAR ir noteiktas vēl vairākas tiesības, kas nav paredzētas Policijas direktīvā, ņemot vērā tās darbības jomu, kas saistīta ar noziedzīgu nodarījumu novēršanu un atklāšanu. VDAR ievieš jaunas tiesības uz datu pārnesamību. To mērķis ir paplašināt datu subjektu iespējas attiecībā uz viņu personas datiem, veicinot viņu spēju viegli pārvietot, kopēt un nosūtīt personas datus no vienas informācijas tehnoloģiju vides uz citu. Tiesības uz datu pārnesamību garantē datu subjektam tiesības saņemt personas datus attiecībā uz sevi, kurus viņš sniedzis pārzinim, strukturētā, plaši izmantotā un mašīnlasāmā formātā un nosūtīt tos citam pārzinim (VDAR 20. panta 1. punkts). Tiesības uz datu pārnesamību ir piemērojamas tikai gadījumā, ja apstrāde tiek veikta ar automatizētiem līdzekļiem. Pārzinim šīs tiesības ir jānodrošina tikai tad, ja personas datu apstrāde ir veikta uz piekrišanas pamata vai tā ir nepieciešama, lai izpildītu līgumu, savukārt tās nav piemērojamas, ja apstrāde tiek veikta, pamatojoties uz citu tiesisko pamatu.

VDAR paredz datu subjektam, balstoties uz iemesliem saistībā ar viņa īpašo situāciju, tiesības jebkurā laikā iebilst pret savu personas datu apstrādi, ja apstrādes tiesiskais pamats ir:

- uzdevumu izpilde, ko veic sabiedrības interesēs vai īstenojot pārzinim piešķirtās oficiālās pilnvaras, vai
- pārziņa vai trešās personas leģitīmo interešu ievērošana (21. panta 1. punkts).

Ja datu subjekts iebilst pret šādu apstrādi, pārzinim ir jāpārvērtē leģitīmo interešu samērīgums ar datu subjekta interesēm (VDAR 21. panta 1. punkts).

Pārzinim ir jāpārtrauc personas datu apstrāde, izņemot, ja tas var norādīt uz pārliecinošiem apstrādes iemesliem, kas ir svarīgāki par datu subjekta pamattiesībām un brīvībām (VDAR 69. apsvērums, 21. panta 1. punkts). Datu subjektam ir tiesības iebilst pret savu personas datu apstrādi tiešās tirgvedības nolūkos, tostarp iebilst pret profilēšanu, ciktāl tā saistīta ar šādu tiešo tirgvedību, gan uzsākot datu apstrādi, gan tās laikā (VDAR 21. panta 2. punkts). Gadījumā, kad persona ir piekritusi datu apstrādei, viņa var izmantot tiesības atsaukt savu piekrišanu jebkurā laikā (VDAR 7. panta 3. punkts), tāpēc tiesības iebilst nav attiecināmas uz apstrādi, kas veikta uz piekrišanas pamata. Ja datu subjekts iebilst pret datu apstrādi tiešās tirgvedības nolūkā, pārzinis personas datus šādam nolūkam vairs nedrīkst apstrādāt (VDAR 21. panta 3. punkts).

Arī VDAR paredz izņēmumus attiecībā uz datu subjekta tiesību ierobežošanu, kā arī datu apstrādes principu ierobežošanu. Saskaņā ar ES un dalībvalstu leģislatīviem pasākumiem, kas piemērojami datu pārzinim un apstrādātājam, var ierobežot pienākumu un tiesību darbības jomu attiecībā uz personas datu apstrādes principiem, datu subjekta tiesībām, kā arī attiecībā uz pārziņa pienākumu ziņot datu subjektam par personas datu aizsardzības pārkāpumiem (VDAR 23. panta 1. punkts). Šādi ierobežojumi ir pieļaujami, ciktāl "tiek ievērota pamattiesību un pamatbrīvību būtība un tas demokrātiskā sabiedrībā ir nepieciešams un samērīgs", lai garantētu būtiskus sabiedrības interešu mērķus: valsts drošību; aizsardzību; sabiedrisko drošību; noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu vai saukšanu pie atbildības par tiem vai kriminālsodu izpildi, tostarp aizsardzību pret sabiedriskās drošības apdraudējumiem un to novēršanu; citus svarīgus ES vai dalībvalsts vispārējo sabiedrības interešu mērķus, datu subjekta aizsardzību vai citu personu tiesību un brīvību aizsardzību u. c. (VDAR 23. panta 1. punkts).

Paredzot šādus ierobežojumus, tiesību aktā ir jāietver arī konkrēti noteikumi vismaz par

- nolūkiem, kādos veic apstrādi, vai par apstrādes kategorijām;
- personas datu kategorijām;
- ieviesto ierobežojumu darbības jomu;
- garantijām, lai novērstu datu ļaunprātīgu izmantošanu vai nelikumīgu piekļuvi vai nosūtīšanu;
- pārziņa vai pārziņu kategoriju noteikšanu;
- glabāšanas laikposmiem un piemērojamām garantijām, ņemot vērā apstrādes vai apstrādes kategoriju raksturu, darbības jomu un nolūku;
- riskiem attiecībā uz datu subjektu tiesībām un brīvībām;
- datu subjektu tiesībām saņemt informāciju par ierobežojumu, izņemot tad, ja tas var kaitēt ierobežojuma mērķim (VDAR 23. panta 2. punkts).

Konvencija 108+ pieļauj izņēmumus no personas datu apstrādes pamatprincipiem un datu subjekta tiesībām, ja šādi izņēmumi ir paredzēti likumā, respektē

pamattiesību un brīvību būtību un ir nepieciešami un samērīgi pasākumi demokrātiskā sabiedrībā, lai

- aizsargātu valsts drošības, aizsardzības, sabiedrības drošības, svarīgas valsts ekonomiskās un finansiālās intereses, tiesu varas objektivitāti un neatkarību vai noziedzīgu nodarījumu novēršanu, izmeklēšanu un kriminālvajāšanu, kā arī kriminālsodu izpildi un citas būtiskas vispārējās sabiedrības intereses;
- aizsargātu datu subjekta vai citu personu tiesības un pamatbrīvības, īpaši vārda brīvību (11. panta 1. punkts).

Tiesību aktā var paredzēt izņēmumus no pārredzamības un informēšanas prasībām, ja dati tiek apstrādāti arhivēšanas nolūkos sabiedrības interesēs, zinātnisko vai vēsturisko pētījumu vai statistikas vajadzībām, ja nepastāv risks, ka tiks pārkāptas datu subjektu tiesības un pamatbrīvības (11. panta 2. punkts). Konvencija 108+ turklāt nosaka, ka, atsaucoties uz apstrādes darbībām valsts drošības un aizsardzības nolūkos, valsts ar likumu var paredzēt izņēmumus arī no citām prasībām, piemēram, kas attiecas uz pārrobežu datu nodošanu, uzraudzības iestāžu pienākumiem un valsts pienākuma atļaut Konvencijas komitejai izvērtēt pasākumu efektivitāti, ciktāl tas ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā, lai sasniegtu šo mērķi. Tas neskar prasību, ka apstrādes darbības valsts drošības un aizsardzības nolūkos tiek pakļautas neatkarīgai un efektīvai pārskatīšanai un uzraudzībai saskaņā ar attiecīgās valsts nacionālajiem tiesību aktiem (11. panta 3. punkts). VDAR, Policijas direktīva un Konvencija 108+ paredz iespējas valstij noteikt daudzus izņēmumus no datu aizsardzības noteikumiem.

Lai nodrošinātu apstrādes likumību un lai izvairītos no patvaļīgas datu apstrādes un iespējamiem pārkāpumiem, īpaša nozīme ir efektīvas uzraudzības un tiesību aizsardzības nodrošināšanai. Tiesību ierobežošanas gadījumā tiesībaizsardzības iestādēm ir jāinformē personas, cita starpā, par piemērotajiem pasākumiem, ja šis paziņojums vairs nespēj apdraudēt šo iestāžu veiktās izmeklēšanas, kā arī par tiesībām iesniegt sūdzību uzraudzības iestādēm un tiesībām uz efektīvu tiesību aizsardzību. Šis pienākums attiecas arī uz datiem, kas tiek apstrādāti, izmantojot sejas atpazīšanas un citas novērošanas tehnoloģijas. Cilvēki var vēlēties apstrīdēt sejas attēla iekļaušanu "novērošanas sarakstā", iebilstot, ka tas darīts nepārredzamā veidā un bez viņu piekrišanas, vai var pieprasīt atlīdzību par viltus pozitīvas atbilstības konstatēšanu, kas viņiem radījusi negatīvas sekas (piemēram, nelikumīga aizturēšana, meklēšana vai arests), tai skaitā pieprasīt atlīdzību par visiem nodarītajiem zaudējumiem (piemēram, ja persona nokavējusi savienoto lidojumu vai viņai nepamatoti liegta iebraukšana ES valstī).[599] Turklāt iespēja vienīgi iesniegt administratīvu sūdzību uzraudzības iestādē netiek

599 FRA (2019), Facial recognition technology.

uzskatīta par efektīvu tiesību aizsardzības līdzekli, piemēram, saskaņā ar Hartas 47. pantu, jo tiesa netiek iesaistīta šādā pārskatīšanā. Ja iekšējie un alternatīvie strīdu izšķiršanas mehānismi izrādās nepietiekami vai ja attiecīgā persona vēlas, lai lieta tiktu pārskatīta tiesā, vienmēr ir jābūt iespējai lietu apstrīdēt tiesā.[600] Lai nodrošinātu iestāžu veiktās apstrādes likumību un novērstu patvaļīgu un pretiesisku datu apstrādi, būtiska nozīme ir atbildības mehānismiem un neatkarīgu iestāžu veiktai šo mehānismu pārraudzībai, no kuriem viens no būtiskākajiem ir ietekmes novērtējums.

6.5. Novērtējums par ietekmi uz datu aizsardzību

Viens no nozīmīgākajiem atbildības mehānismiem, kas ir noteikts ES datu aizsardzības tiesību aktos, ir novērtējums par ietekmi uz datu aizsardzību. Tas ļauj novērtēt apstrādes darbības, to iespējamos riskus attiecībā uz personu tiesībām un brīvībām, kā arī noteikt pasākumus šo risku mazināšanai un novēršanai.

VDAR nosaka, ka novērtējums ir obligāti jāveic, ja plānotās apstrādes darbības varētu radīt augstu risku fizisku personu tiesībām un brīvībām (35. panta 1. punkts). VDAR 35. panta 3. punkts nosaka kritērijus, kad novērtējums ir īpaši vajadzīgs. Tie ir:

1) ar fiziskām personām saistītu personisku aspektu sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde, tostarp profilēšana, un ar kuru pamato lēmumus, kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu;
2) īpašo kategoriju datu vai personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā;
3) publiski pieejamas zonas sistemātiska uzraudzība plašā mērogā.

Līdzās minētajiem gadījumiem apstrāde var radīt augstu risku arī citos gadījumos, un pārzinim var būt pienākums veikt novērtējumu. 29. panta darba grupa ir noteikusi deviņus kritērijus, kas jāņem vērā pārziņiem, novērtējot, vai apstrādes darbības "varētu radīt augstu risku" un attiecīgi vai ir veicams novērtējums. Šie kritēriji ir:

1) vērtēšana vai punktu piešķiršana, tostarp profilēšana un prognozes;
2) automatizēti lēmumi, kuriem ir tiesiskas vai līdzīgi būtiskas sekas;
3) sistemātiska novērošana;
4) sensitīvi vai ļoti personiska rakstura dati;
5) datu apstrāde plašā mērogā;
6) datu kopu saskaņošana vai apkopošana;

600 FRA (2019), Facial recognition technology.

7) dati par neaizsargātiem datu subjektiem;
8) jaunu tehnoloģisko vai organizatorisko risinājumu izmantošana vai piemērošana;
9) ja apstrāde kavē datu subjektus īstenot savas tiesības vai izmantot pakalpojumu vai līgumu.

Vairākumā gadījumu datu pārzinis var uzskatīt, ka tad, ja apstrāde atbilst diviem kritērijiem, attiecībā uz to ir jāveic novērtējums, un, jo vairāk kritērijiem apstrāde atbilst, jo lielāka ir varbūtība, ka tā radīs augstu risku datu subjektu tiesībām un brīvībām.[601] Uzraudzības iestādēm ir jāizstrādā un jāpublisko saraksts ar tām apstrādes darbībām, kurām ir jāveic novērtējums, un tās arī var izstrādāt sarakstu ar apstrādes darbībām, kam novērtējums nav jāveic (VDAR 35. panta 4. un 5. punkts).[602]

VDAR turklāt paredz, ka valsts tiesību aktos var būt noteikts, ka pārzinim ir jāapspriežas ar uzraudzības iestādi un jāsaņem no tās iepriekšēja atļauja saistībā ar apstrādi, ko tas veic, lai izpildītu sabiedrības interesēs īstenojamu uzdevumu, tostarp, kad minēto apstrādi veic saistībā ar sociālo aizsardzību un sabiedrības veselību (36. panta 5. punkts).

Pārzinis var izmantot dažādas metodoloģijas novērtējuma veikšanai. ES dalībvalstu uzraudzības iestādes ir publicējušas dažādas vadlīnijas, kā arī tiešsaistes rīkus[603], lai palīdzētu uzņēmumiem un organizācijām sagatavot novērtējumus. VDAR 35. panta 7. punkts nosaka, ka novērtējumā ietver vismaz

a) plānoto apstrādes darbību un apstrādes nolūku, tostarp attiecīgā gadījumā pārziņa leģitīmo interešu sistemātisku aprakstu;
b) novērtējumu par apstrādes darbību nepieciešamību un samērīgumu attiecībā uz nolūkiem;
c) novērtējumu par riskiem datu subjektu tiesībām un brīvībām;
d) pasākumus, kas paredzēti risku novēršanai, tostarp garantijas, drošības pasākumus un mehānismus, ar ko nodrošina personas datu aizsardzību

601 Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/611236/en

602 Sk. Datu valsts inspekcija. (2018). Apstrādes darbību veidi, attiecībā uz kuriem ir jāveic datu aizsardzības ietekmes novērtējums saskaņā ar VDAR 35. panta 4. punktu. https://www.dvi.gov.lv/lv/media/92/download

603 Sk., piemēram, ICO. Data Protection Impact Assessments (DPIAs). https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/; CNIL. (2019). The open source PIA softwere helps to carry out data protection impact assessment. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

un uzskatāmi parāda, ka ir ievērota VDAR, ņemot vērā datu subjektu un citu attiecīgo personu tiesības un leģitīmās intereses.

Pārzinim ir jālūdz padoms datu aizsardzības speciālistam, ja tāds ir iecelts (VDAR 35. panta 2. punkts), piemēram, par šādiem jautājumiem: ir vai nav jāveic novērtējums; kāda metodika ir jāizmanto; kādi drošības pasākumi ir jāveic, lai mazinātu datu subjektu tiesību un interešu risku; vai novērtējums ir veikts pareizi; vai secinājumi atbilst VDAR u. c.[604]

Policijas direktīva arī nosaka pienākumu veikt novērtējumu par ietekmi uz datu aizsardzību. Ja apstrādes veids, jo īpaši izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus, varētu radīt augstu risku fizisko personu tiesībām un brīvībām, valsts paredz, ka pārzinis pirms apstrādes veic novērtējumu par to, kā plānotās apstrādes darbības ietekmēs personas datu aizsardzību (27. panta 1. punkts). Šajā novērtējumā ietver vismaz plānoto apstrādes darbību vispārīgu aprakstu, novērtējumu par riskiem datu subjektu tiesībām un brīvībām, pasākumus, kas paredzēti minēto risku novēršanai, garantijas, drošības pasākumus un mehānismus, ar kuriem nodrošina personas datu aizsardzību un uzskatāmi parāda, ka ir ievērota Policijas direktīva, ņemot vērā datu subjektu un citu attiecīgo personu tiesības un leģitīmās intereses (27. panta 2. punkts).

Gan VDAR, gan Policijas direktīva paredz iepriekšēju apspriešanos ar uzraudzības iestādi. VDAR nosaka – ja novērtējumā tiek konstatēts, ka gadījumā, ja pārzinis neveiktu pasākumus riska mazināšanai, apstrāde radītu augstu risku, pārzinim pirms apstrādes ir jāapspriežas ar uzraudzības iestādi (36. panta 1. punkts). Ja uzraudzības iestāde uzskata, ka plānotā apstrāde pārkāptu VDAR, it īpaši tad, ja pārzinis nav pietiekami identificējis vai mazinājis risku, tā sniedz pārzinim un attiecīgā gadījumā apstrādātajam rakstisku padomu un var izmantot citas izmeklēšanas pilnvaras (36. panta 2. punkts). Apspriežoties ar uzraudzības iestādi, pārzinis sniedz tai nepieciešamo informāciju par apstrādi, tās nolūkiem, līdzekļiem, pasākumiem un garantijām, lai nodrošinātu datu subjektu tiesību un brīvību aizsardzību saskaņā ar VDAR (36. panta 3. punkts).

Policijas direktīva savukārt nosaka, ka valsts paredz pienākumu pārzinim vai apstrādātājam apspriesties ar uzraudzības iestādi pirms tādu personas datu apstrādes, ko ietvers jaunizveidotā kartotēkā, ja

1) novērtējumā par ietekmi uz datu aizsardzību ir norādīts, ka gadījumā, ja pārzinis neveiktu pasākumus riska mazināšanai, apstrāde radītu augstu risku; vai

604 Article 29 Data Protection Working Party (2016), Guidelines on Data Protection Officers ('DPOs').

2) apstrādes veids, jo īpaši tāds, kurā izmantotas jaunas tehnoloģijas, mehānismi vai procedūras, ir saistīts ar augstu risku datu subjektu tiesībām un brīvībām (28. panta 1. punkts).

Pārzinim ir jāiesniedz uzraudzības iestādei novērtējums par ietekmi uz datu aizsardzību un pēc pieprasījuma jebkura cita informācija, kas ļauj tai izvērtēt apstrādes atbilstību, jo īpaši riskus datu subjekta personas datu aizsardzībai un attiecīgās garantijas (28. panta 4. punkts).

Lai gan Konvencija 108+ neparedz ietekmes novērtējumu kā atsevišķu atbildības mehānismu, tajā ir noteikts, ka valsts nodrošina, ka pārziņi un attiecīgā gadījumā apstrādātāji pirms datu apstrādes uzsākšanas pārbauda paredzētās datu apstrādes iespējamo ietekmi uz datu subjektu tiesībām un pamatbrīvībām un plāno datu apstrādi tā, lai novērstu vai samazinātu risku iejaukties šajās tiesībās un pamatbrīvībās (10. panta 2. punkts).

Sejas atpazīšanas tehnoloģiju izmantošanas gadījumā pārzinim ir jāveic novērtējums par ietekmi uz datu aizsardzību.[605] VDAR 35. pantā un Policijas direktīvas 28. pantā noteiktie kritēriji, kas ļauj izvērtēt, vai ir jāveic novērtējums, īpaši saistībā ar jauno tehnoloģiju izmantošanu, lielā mērā ir attiecināmi uz sejas atpazīšanas tehnoloģiju izmantošanu. Datu valsts inspekcijas publicētajā sarakstā ar tām apstrādes darbībām, attiecībā uz kurām ir jāveic novērtējums, ir ietverta arī "inovatīva jaunu tehnoloģiju vai risinājumu izmantošana vai to pielietošana, piemēram, apvienojot pirkstu nospiedumu un sejas atpazīšanas lietošanu, lai uzlabotu piekļuves kontroli utt."[606] VDAR turklāt paredz, ka novērtējums ir īpaši vajadzīgs, apstrādājot īpašu kategoriju personas datus vai personas datus par sodāmību un pārkāpumiem plašā mērogā (35. panta 3. punkta b) apakšpunkts), kā arī veicot publiski pieejamu zonu uzraudzību plašā mērogā (35. panta 3. punkta c) apakšpunkts). Sejas atpazīšanas tehnoloģijas ietver biometrisko datu apstrādi, un to izmantošanas nolūks var būt saistīts ar publiskas telpas uzraudzību plašā mērogā. Novērtējuma veikšana pirms apstrādes uzsākšanas ļauj noteikt, vai konkrētajā gadījumā sejas atpazīšanas tehnoloģijas izmantošana ir pieļaujama.

Pirms jaunu tehnoloģiju ieviešanas, ja to veiktā personas datu apstrāde var aizskart personu pamattiesības, ir jāiesaista uzraudzības iestāde. Gan VDAR, gan Policijas direktīva paredz, ka valsts apspriežas ar uzraudzības iestādi, kamēr tiek gatavots priekšlikums leģislatīvam pasākumam, ko pieņems valsts parlaments, vai regulatīvs pasākums, kas balstās uz šādu leģislatīvu pasākumu, kurš attiecas uz apstrādi (VDAR 36. panta 4. punkts, Policijas direktīvas 28. panta 2. punkts). Turklāt datu aizsardzības novērtējums atsevišķos gadījumos var nebūt pietiekams, jo līdzās riskiem datu subjekta tiesībām un brīvībām var būt jāvērtē to plašāka

605 EDPB (2019), Guidelines 3/2019 on processing of personal data through video devices.

606 Sk. Datu valsts inspekcija (2018), Apstrādes darbību veidi, attiecībā uz kuriem ..

ietekme uz sabiedrību un demokrātiju. Lai gan Latvijā sejas atpazīšanas tehnoloģijas sabiedriskās vietās nav ieviestas, Iekšlietu ministrija ir apsvērusi iespēju izveidot vienotu videonovērošanas kameru tīklu ar sejas atpazīšanas programmatūru.[607] Pirms jaunu novērošanas tehnoloģiju ieviešanas ir būtiski noskaidrot gan Datu valsts inspekcijas, gan citu tiesībaizsardzības iestāžu, piemēram, Tiesībsarga biroja, viedokli. Tāpat svarīgi ir uzzināt personu, kuru dati tiks apstrādāti, viedokli. VDAR paredz, ka attiecīgā gadījumā pārzinim ir jāprasa datu subjektu vai viņu pārstāvju viedoklis par plānoto apstrādi, izvērtējot šādu iepriekšēju konsultēšanās nepieciešamību katrā konkrētajā gadījumā (35. panta 9. punkts). Policijas direktīva šādu prasību neparedz. Tajā pašā laikā tādu tehnoloģiju ieviešana, kas būtiski ierobežo cilvēktiesības, nedrīkstētu notikt bez sabiedrības viedokļa uzklausīšanas un tās atbalsta.

Nākamā grāmatas nodaļa veltīta ieteikumiem, kā attīstīt mākslīgā intelekta novērošanas tehnoloģiju regulējumu, atbildības un uzraudzības mehānismus. Bet vispirms sniegts ieskats, kā datu aizsardzības standarti tika attiecināti uz kontakta izsekošanas lietotnēm, kas bija viena no tehnoloģijām, kuru ieviesa cīņā ar koronavīrusa pandēmiju. Tās izvērtējums var palīdzēt attīstīt uzraudzības mehānismus un regulējumu arī attiecībā uz citām tehnoloģijām, tostarp mākslīgā intelekta novērošanas tehnoloģijām.

6.6. Datu aizsardzības standarti kontaktu izsekošanas lietotnēm

Lai novērstu sabiedrības bažas par personas datu prettiesisku izmantošanu un atbalstītu valstis un lietotņu izstrādātājus, daudzas starptautiskas, ES un valstu iestādes izstrādāja vadlīnijas, kas skaidro datu aizsardzības prasības kontaktu izsekošanas lietotnēm. 2020. gada 16. aprīlī Eiropas Komisija publicēja divas pamatnostādnes, lai atbalstītu vienotu koordinētu pieeju kontaktu izsekošanas lietotņu izmantošanai visās ES valstīs. ES dalībvalstu e-veselības tīkls ar Eiropas Komisijas atbalstu izstrādāja ES rīkkopu mobilo lietojumprogrammu izmantošanai kontaktu izsekošanai un brīdināšanai.[608] Kopā ar rīkkopu Eiropas Komisija pieņēma Norādījumus par lietotnēm, kas sniedz atbalstu cīņā pret Covid-19

607 Spundiņa, L. (1. oktobris 2020). Datu valsts inspekcija neatbalsta sejas atpazīšanas videonovērošanas iekārtas. *LSM.lv*. https://www.lsm.lv/raksts/zinas/latvija/datu-valsts-inspekcija-neatbalsta-sejas-atpazisanas-videonoverosanas-iekartas.a376399/

608 E-health Network. (2020). Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States. https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19_apps_en.pdf

pandēmiju saistībā ar datu aizsardzību.[609] 2020. gada 21. aprīlī Eiropas Datu aizsardzības kolēģija pieņēma pamatnostādnes par atrašanās vietas datu un kontaktu izsekošanas rīku izmantošanu saistībā ar Covid-19 uzliesmojumu.[610] Šajos dokumentos ir noteikti datu aizsardzības standarti kontaktu izsekošanas lietotnēm, lai tās atbilstu ES datu aizsardzības regulējumam.

Arī citas starptautiskas organizācijas pieņēma vairākas vadlīnijas. 2020. gada 21. aprīlī Eiropas Padome publicēja kopīgu paziņojumu par digitālo kontaktu izsekošanu.[611] OECD 2020. gada 23. aprīlī publicēja dokumentu par Covid-19 izsekošanu un privātuma un datu aizsardzību, izmantojot lietotnes un biometriskos datus.[612]

Šie dokumenti nosaka kopīgas minimālās datu aizsardzības prasības kontaktu izsekošanas lietotnēm. FRA veiktajā pētījumā ir norādīts, ka visos vai lielākajā daļā no iepriekš minētajiem dokumentiem ir noteiktas šādas prasības:

1) pierādīta efektivitāte pirms izstrādes;
2) brīvprātīgums;
3) iepriekšējs ietekmes novērtējums;
4) integrēta datu aizsardzība;
5) noteikts mērķis un juridiskais pamats;
6) atvērtais pirmkods un pārredzamība;
7) datu minimizēšana un precizitāte;
8) kontaktu noteikšanas tehniskā precizitāte;
9) anonīmi un pseidonimizēti dati;
10) drošība pret kiberuzbrukumiem;
11) atrašanās vietas datu neapstrādāšana;
12) regulāra neatkarīga uzraudzība;
13) savstarpējā savietojamība;

609 Eiropas Komisija. (2020). Komisijas paziņojums. Norādījumi par lietotnēm, kas sniedz atbalstu cīņā pret Covid-19 pandēmiju saistībā ar datu aizsardzību. *OV C* 124/1, 17.04.2020. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020XC0417(08)&from=EN

610 Eiropas Datu aizsardzības kolēģija. (2020). Pamatnostādnes 04/2020 par atrašanās vietas datu un kontaktu izsekošanas rīku izmantošanu saistībā ar Covid-19 uzliesmojumu. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_lv.pdf

611 Council of Europe. (2020). Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7

612 OECD. (2020). Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics. https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics/

14) deaktivizēšana un dzēšana pēc pandēmijas;
15) dalībnieku atbildība.[613]

Teorētiski kontaktu izsekošanas lietotnēm būtu jāatbilst visām šīm datu aizsardzības prasībām. Tomēr, lai gan valstu starpā pastāvēja vienprātība par daļu no prasībām, piemēram, brīvprātīgumu un īslaicīgumu, dažas prasības netika ievērotas vai tika izmantotas atšķirīgas pieejas. Piemēram, kas attiecas uz prasību pēc tiesību aktiem, dažas ES valstis izstrādāja speciālus tiesību aktus kontaktu izsekošanas lietotnēm, lai nodrošinātu juridisko pamatu un precizētu personu datu apstrādi, kā arī lai valsts iestādes varētu ieviest un izmantot lietotnes. Tomēr daudzās valstīs šāda likumdošana netika izstrādāta, un dažas valstis arī noliedza tās nepieciešamību.[614]

Lai nodrošinātu atbilstību datu aizsardzības regulējumam, viena no prasībām ir veikt kontaktu izsekošanas lietotnes ietekmes uz datu aizsardzību novērtējumu un to publiskot. Eiropas Datu aizsardzības kolēģija norāda, ka ir jāveic novērtējums pirms šo lietotņu ieviešanas, jo tās ietver veselības datu plašu apstrādi, sistemātisku uzraudzību un jaunu tehnoloģisku risinājumu izmantošanu, kas var radīt augstu risku personu tiesībām un brīvībām.[615] Būtiska prasība ir arī datu aizsardzības iestāžu iepriekšēja un pastāvīga iesaistīšanās kontaktu izsekošanas lietotņu izstrādē un novērtēšanā. Lai gan vairākums ES valstu, to skaitā Latvija pirms lietotnes "Apturi Covid" ieviešanas, konsultējās ar datu aizsardzības iestādēm par lietotņu izmantošanu, daudzas valstis iepriekš neveica ietekmes uz datu aizsardzību novērtējumu. Iepriekšēja novērtējuma trūkums rada bažas par pārredzamības, pārskatatbildības, datu aizsardzības un privātuma prasību ievērošanu.[616]

Dažas ES un starptautisko organizāciju ieteiktās prasības var pārsniegt datu aizsardzības regulējuma prasības, piemēram, prasība pēc atvērtā pirmkoda un publiski pieejama ietekmes novērtējuma, bet tās palīdz nodrošināt pārredzamību.[617] Augsts pārredzamības līmenis ir būtisks kontaktu izsekošanas lietotņu akceptēšanai sabiedrībai, sabiedrības kontrolei un uzticības veicināšanai.

Jebkuras kontaktu izsekošanas lietotnes efektivitāte ir atkarīga no plaša sabiedrības atbalsta. Viena no galvenajām problēmām ir nodrošināt, ka lietotnes izmanto plaša sabiedrības daļa. Sabiedrības atbalstu var veicināt, izvēloties datu minimizēšanas prasībām atbilstošāko risinājumu.

613 FRA (2020), Coronavirus pandemic in the EU ..

614 Ibid.

615 Eiropas Datu aizsardzības kolēģija (2020), Pamatnostādnes 04/2020 ..

616 FRA (2020), Coronavirus pandemic in the EU ..

617 Eiropas Datu aizsardzības kolēģija (2020), Pamatnostādnes 04/2020 ..

Jaunās pieejas datu vākšanai un apstrādei kontaktu izsekošanas lietotnēs radīja plašas diskusijas. Atbilstoši vadlīnijās sniegtajiem ieteikumiem lielākajā daļā ES valstu, ieskaitot Latviju, kontaktu izsekošanas lietotnes darbojās, izmantojot *Bluetooth* tehnoloģiju, kas ļauj konstatēt savienojumu starp ierīcēm, tomēr dažās valstīs tika izmantoti arī atrašanās vietas dati. Piemēram, Norvēģija apturēja savu kontaktu izsekošanas lietotni pēc tam, kad datu aizsardzības iestāde paziņoja, ka tā rada nesamērīgus draudus lietotāju privātumam, tostarp izmantojot atrašanās vietas datus.[618]

Kontaktu izsekošanas lietotnes var balstīt uz centralizētu vai decentralizētu pieeju. Lielākā daļa ES valstu, arī Latvija, izvēlējās decentralizētu pieeju, kur lietotāju dati tiek saglabāti viņu ierīcēs, tomēr dažās valstīs, piemēram, Francijā, tika ieviestas lietotnes ar centralizētu pieeju, kur lietotāju dati tiek glabāti un apstrādāti centrālajā serverī.[619] Lai gan Eiropas Komisija un Eiropas Datu aizsardzības kolēģija nav devusi priekšroku nevienai no abām pieejām, tiek uzskatīts, ka decentralizētais risinājums vairāk atbilst datu minimizēšanas principam.

Lielākā daļa ES dalībvalstu, izstrādājot nacionālās kontaktu izsekošanas lietotnes, izmantoja publiski pieejamus protokolus. Pirmā tika piedāvāta Viseiropas privātuma saglabāšanas tuvuma izsekošanas (PEPP-PT) iniciatīva, kas paredzēja centralizētu mehānismu, tai sekoja decentralizēta alternatīva (DP-3T). Pēc tam "Apple" un "Google" paziņoja, ka izstrādās lietojumprogrammu saskarni (*Exposure Notification API* – angļu val.), pamatojoties uz decentralizētu pieeju, kā arī norādīja, ka tā neatbalstīs centralizētu lietotņu arhitektūru. Kaut arī daudzas valstis sākotnēji izvēlējās centralizētu pieeju, pēc "Apple" un "Google" paziņojuma vairākas valstis, tostarp Lielbritānija, Itālija un Vācija, atteicās no centralizētas lietotnes ieviešanas un nolēma atbalstīt šo decentralizēto pieeju. Daudzas citas Eiropas valstis, ieskaitot Latviju, Igauniju, Somiju, Austriju, Īriju, Čehiju un Šveici, arī ieviesa lietotnes, kuru pamatā ir "Apple" un "Google" decentralizētais modelis.[620] Turklāt "Apple" operētājsistēmas iOS 13.7 atjauninājumā ieviesa funkciju *Exposure Notification Express,* kas ļauj *iPhone* lietotājiem veikt kontaktu izsekošanu bez nepieciešamības lejupielādēt oficiālu Covid-19 lietotni.[621] Iepriekš

618 Manancourt (15 June, 2020), Norway suspends contact-tracing app over privacy concerns.

619 European Commission. (2020). Mobile applications to support contact tracing in the EU's fight against COVID-19. Progress reporting June 2020. https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf

620 Sk. Rahman, M. (25 February, 2021). Here are the countries using Google and Apple's COVID-19 Contact Tracing API. *XDA Developers.* https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/

621 Kelion, L. (1 September, 2020). Coronavirus: Apple iPhones can contact-trace without Covid app. *BBC News*. https://www.bbc.com/news/technology-53987928

minētās epizodes spilgti parāda ASV tehnoloģiju gigantu ietekmi uz valdību lēmumiem,[622] strauji pieaugošo valstu atkarību no tiem, ieviešot plaša mēroga digitālos risinājumus sabiedrības interesēs, un tas rada tālākus jautājumus par šo lielo tehnoloģiju uzņēmumu varas ierobežošanu un digitālās suverenitātes aizsardzību.

Neatkarīgi no izvēlētā tehnoloģiskā risinājuma galvenais jautājums, kas jāuzdod saistībā ar kontakta izsekošanas lietotnēm, kā arī ikvienu citu digitālo risinājumu izmantošanu, ir – vai šie risinājumi var palīdzēt apturēt vīrusa izplatību, proti, vai tie ir efektīvi. Šo lietotņu efektivitāte ir atkarīga no tā, cik daudz iedzīvotāju to ir lejupielādējuši un izmanto. Oksfordas Universitātes pētnieki norāda, ka vismaz 60 % iedzīvotāju būtu jāizmanto lietotne, lai tā būtu efektīva.[623] Lietotnes, kas vairs nav efektīvas, ir jāuzlabo, vai to darbība jāpārtrauc. Ja digitālās novērošanas tehnoloģijas ir neefektīvas, tās kļūst nevajadzīgas, un tādējādi arī to izmantošana ir uzskatāma par prettiesisku. Šo digitālo tehnoloģiju efektivitāte, lai palīdzētu ierobežot Covid-19 izplatību, tā arī netika pierādīta.[624]

Kontaktu izsekošanas lietotņu un citu jauno tehnoloģiju ietekmes, efektivitātes un nepieciešamības novērtēšana un stingra pārraudzība gan pandēmijas laikā, gan pēc tās ir būtiska, ne tikai lai palīdzētu aizsargāt cilvēktiesības, bet arī lai masveida novērošanas pasākumi nekļūtu par jauno normu. Tas, cik ātri plašs ieinteresēto dalībnieku – zinātnieku, tehnoloģiju uzņēmumu, civilo sabiedrības organizāciju, starptautisko organizāciju – loks tika iesaistīts un sadarbojās, lai izstrādātu standartus kontaktu izsekošanas lietotņu ieviešanai un lai izvērtētu to darbību, varētu būt labs piemērs praksei, kā varētu tikt izvērtēta arī citu jauno tehnoloģiju atbilstība regulējumam. Daudzas prasības, kas izkristalizējās diskusiju laikā, piemēram, efektivitāte, brīvprātīgums, ietekmes novērtējums, neatkarīga uzraudzība, termiņa ierobežošana, atbildība, ir būtiski attiecināt arī uz mākslīgā intelekta novērošanas tehnoloģijām.

Nākamajā nodaļā sniegtas konkrētas politikas rekomendācijas, vēršot uzmanību uz nepieciešamību ne tikai nodrošināt atbildības un uzraudzības prasības, bet arī paredzēt stingrus ierobežojumus šo tehnoloģiju izmantošanai.

622 Sk. Ilves, I. (16 June, 2020). Why are Google and Apple dictating how European democracies fight coronavirus? *The Guardian.* https://www.theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-european-democracies-coronavirus

623 Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown. (16 April, 2020). *University of Oxford.* https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

624 Sk., piemēram, European Commission (2020), Mobile applications to support contact tracing ..

7. DAĻA

Mākslīgā intelekta novērošanas regulējuma izstrāde un sarkanās līnijas: politikas rekomendācijas

Grāmatas iepriekšējās nodaļās atklāts, cik lielu apdraudējumu mākslīgā intelekta novērošanas tehnoloģijas rada cilvēktiesībām un demokrātijai. Tāpat parādīts, kā esošais cilvēktiesību un datu aizsardzības regulējums ir piemērojams attiecībā uz šīm tehnoloģijām, kā tas attīstās un kādus tiesiskos izaicinājumus tās rada. Šajā nodaļā sniegti vairāki ieteikumi, kā attīstīt tālāk mākslīgā intelekta regulējumu un kādi līdzekļi un aizsardzības garantijas ir jāievieš praksē, lai nodrošinātu atbildīgu un uzticamu mākslīgā intelekta tehnoloģiju izmantošanu, kas novērstu to radītos riskus un aizsargātu cilvēktiesības, demokrātiju un tiesiskumu.

Vispirms atklāts, ka mākslīgā intelekta regulējums nav saistīts tikai ar ētikas principiem, un uzsvērts, ka šī regulējuma turpmākajā attīstībā visnozīmīgākās ir cilvēktiesības. Pēc tam pamatots, ka, lai novērstu mākslīgā intelekta novērošanas tehnoloģiju radītos riskus, ir nepieciešams steidzami pieņemt mākslīgā intelekta tiesisko regulējumu, kas cita starpā noteiktu šo tehnoloģiju izmantošanas sarkanās līnijas. Tālāk ieteikti vairāki būtiski mehānismi un aizsardzības garantijas: mākslīgā intelekta ietekmes novērtējums, neatkarīga uzraudzība, sabiedrības līdzdalība, pārredzamības un informēšanas prasības. Nobeigumā vērsta uzmanība – lai masveida novērošana nekļūtu par jauno normu, ir stingri jāuzrauga to novērošanas tehnoloģiju izmantošana, kuras valstis strauji ieviesa cīņā ar Covid-19.

7.1. No ētikas principiem līdz to ieviešanai praksē

Diskusijās par mākslīgā intelekta regulējumu līdz šim lielākā uzmanība ir pievērsta ētikas principiem. Pētījumi, kuros ir salīdzinātas un analizētas mākslīgā intelekta ētikas vadlīnijas, ko pieņēmušas starptautiskās organizācijas, nevalstiskās un profesionālās organizācijas, kā arī tehnoloģiju uzņēmumi, parāda, ka lielā mērā pastāv konverģence starp tajās noteiktajiem ētiskajiem principiem, piemēram, privātumu, atbildību, pārredzamību, cilvēka kontroli pār tehnoloģijām, taisnīgumu un nediskrimināciju.[625]

Vienlaikus ir arī konstatēts, ka šīs vadlīnijas, kuru skaits jau 2020. gadā bija tuvu simtam un turpina pieaugt, lielākoties sniedz vispārējus ieteikumus un

625 Sk. Fjeld, et al. (2020), Principled Artificial Intelligence; Jobin, Ienca, Vayena (2019), The global landscape of AI ethics guidelines.

priekšlikumus, bet neparedz praktiskus izpildes mehānismus.[626] Turklāt pastāv būtiskas atšķirības, kā šie principi tiek interpretēti un īstenoti praksē.[627] Ir daudz politiska un tiesiska rakstura neskaidrību, un tiek piedāvāti dažādi un bieži vien pretrunīgi pasākumi, kā praktiski nodrošināt uz ētikas principiem balstīta mākslīgā intelekta attīstību.[628]

Šī atšķirīgā izpratne par dažādiem principiem, tostarp privātuma un datu aizsardzības prasībām, un to piemērošanu praksē, par to, kā samērojamas konkurējošas intereses, traucē vienoties par globālu regulējumu.[629] Organizācijas, kas uzņemas vadību mākslīgā intelekta regulējuma izstrādē, var to veidot atbilstīgi savām interesēm, un tām ir labākas iespējas pielāgot regulējumu savām vajadzībām. Ņemot vērā mākslīgā intelekta ētikas un satura neskaidrību un elastību, patlaban ikviens šo regulējumu var veidot ar sev vēlamo ētisko saturu.[630]

Turklāt starp dažādiem ētikas principiem ir iespējami konflikti, kas prasa vienotu pieeju, kā tos risināt. Konflikts var pastāvēt, piemēram, starp privātuma un pārredzamības prasību. Viena no pretrunām rodas starp prasību izvairīties no iespējamā kaitējuma un prasību līdzsvarot riskus un ieguvumus. Turklāt risku un ieguvumu novērtējums var novest pie atšķirīgiem rezultātiem atkarībā no interesēm, kuras tiek pārstāvētas. Sabiedrības intereses var netikt ņemtas vērā, līdzsvarojot konkurējošas prasības, piemēram, gadījumos, kad tiek ietekmētas ētiskas vērtības, bet tajā pašā laikā tiek iegūtas arī ekonomiskas vai politiskas priekšrocības.[631] Ja šādi konflikti netiek atrisināti, var būt apgrūtināti centieni izstrādāt globālu mākslīgā intelekta ētikas regulējumu. Bez būtiskām izmaiņām regulējumā ētikas principu ieviešana praksē paliks konkurējošs, nevis sadarbības process.[632]

Kā tika atklāts grāmatas piektajā nodaļā, ir izstrādāta plaša starptautiskā tiesu prakse un izveidota strukturēta sistēma konfliktu risināšanai starp konkurējošām cilvēktiesībām un sabiedrības interesēm, piemēram, privātuma un drošības

626 Hagendorff, T. (2020). The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds & Machines,* 30, 99–120. https://doi.org/10.1007/s11023-020-09517-8

627 Ryan, M., Stahl, B. C. (2020). Artificial Intelligence Ethics Guidelines for Developers and Users: Clarifying Their Content and Normative Implications, *Journal of Information, Communication and Ethics in Society,* 19(1). https://doi.org/10.1108/JICES-12-2019-0138

628 Jobin, Ienca, Vayena (2019), The global landscape of AI ethics guidelines.

629 Ibid.

630 Yeung, K., Howes, A., Pogrebna, G. (2020). AI Governance by Human Rights–Centered Design, Deliberation, and Oversight: An End to Ethics Washing, p. 80. In: Dubber, M. D., Pasquale, F., and Das, S. (eds.), *The Oxford Handbook of Ethics of AI*, 75–106. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190067397.013.5

631 Mittelstadt (2019), Principles alone cannot guarantee ethical AI.

632 Ibid.

interesēm. Konfliktu risināšana starp dažādām cilvēktiesībām ir labi saprotama, un to plaši piemēro cilvēktiesību juristi, jo tā veido būtisku daļu no cilvēktiesību piemērošanas prakses. Kā tika atklāts iepriekš grāmatas piektajā nodaļā, pastāv vairāki pamatnosacījumi cilvēktiesību ierobežošanai, it īpaši prasība, ka ierobežojumiem ir jābūt skaidri noteiktiem likumā un tie nevar pārsniegt minimumu, kas ir nepieciešams, lai sasniegtu konkrēto sabiedrības mērķi.[633] Šī sistēma būtu piemērojama arī attiecībā uz konfliktu risināšanu starp ētikas normām, kas prasa samērot pretējās intereses, izvērtējot to nepieciešamību un proporcionalitāti.

Mākslīgā intelekta attīstību nevar balstīt vienīgi uz mākslīgā intelekta ētikas principiem.[634] Vienoties par kopīgām un starptautiski atzītām morāles normām un ideāliem ir svarīgi, jo tie tiecas uz pilnību, iedvesmo uz rīcību, iezīmē skaidrāku virzību tāda mākslīgā intelekta attīstībai, kas kalpotu cilvēcei un sabiedrībai un sniegtu ieguvumus. Tomēr ar tiem nav pietiekami. Vienlaikus ir jānosaka arī metodes un līdzekļi, kas ļauj ētikas vērtības un principus ieviest praksē.

Tiesiskās prasības ir svarīgs instruments, lai nodrošinātu atbildību un ieviestu praksē ētikas principus un sociālās vērtības. Lai gan pastāv pamatotas domstarpības par to, kas ir ētiska rīcība katrā konkrētā gadījumā, ir jādefinē saskaņotu normu kopums, kas veido minimālās prasības, kuras jāievēro, lai mākslīgā intelekta sistēmu izstrādi, ieviešanu un izmantošanu varētu atzīt par ētisku un likumīgu.[635] Ir nepieciešams izstrādāt skaidru tiesisko regulējumu, kas atbilstu ētikas normām un cilvēktiesībām.

Juridiski saistošas prasības un pienākumi ir īpaši svarīgi gadījumos, kad mākslīgā intelekta sistēmas var radīt augstu risku un būtisku apdraudējumu. Šādā gadījumā nepietiek ar brīvprātīgām prasībām, lai novērstu radītos riskus. Skaidrs tiesiskais regulējums ir sevišķi nepieciešams attiecībā uz mākslīgā intelekta masveida novērošanas tehnoloģiju izstrādi, ieviešanu un izmantošanu, ņemot vērā to radīto būtisko apdraudējumu.

Cilvēktiesības ir pamatā ētikas principiem. To ievērošana demokrātiskā un tiesiskā sabiedrībā ir visdrošākais pamats abstrakto ētikas principu un vērtību noteikšanai. Cilvēktiesības ietver skaidri definētus jēdzienus un uzliek skaidrus juridiskus pienākumus, kas ir noteikti starptautiskajos tiesību aktos. Starptautiskie cilvēktiesību standarti piedāvā visprecīzāko ētikas normu kopumu mākslīgā intelekta sistēmām.[636] Vienlaikus arī ētikas principu formulēšana papildina cilvēktiesību standartus. Šie principi var palīdzēt saprast, kā mākslīgā intelekta izstrāde, ieviešana un izmantošana varētu ietekmēt cilvēktiesības un to pamatā

633 Yeung, Howes, Pogrebna (2020), AI Governance by Human Rights .., p. 83.

634 Mittelstadt (2019), Principles alone cannot guarantee ethical AI.

635 Yeung, Howes, Pogrebna (2020), AI Governance by Human Rights .., p. 80.

636 Ibid., pp. 80–81.

esošās vērtības, likt apsvērt ne tikai to, kā mēs tehnoloģijas varētu izmantot, bet gan arī to, kādā veidā mums tehnoloģijas būtu jāizmanto, lai tās sniegtu labumu, nevis apdraudētu sabiedrību.[637]

7.2. Cilvēktiesības kā mākslīgā intelekta regulējuma stūrakmens

Cilvēktiesības ir stūrakmens ētiskai un uz cilvēku vērstai mākslīgā intelekta regulējuma turpmākai attīstībai. Starptautiskās cilvēktiesības veido starptautisku tiesību kopums, kā arī reģionālās cilvēktiesību sistēmas, kas ir izveidotas pēdējo 70 gadu laikā visā pasaulē. Kā starptautisks pārvaldības mehānisms cilvēktiesību tiesiskais regulējums ir paredzēts, lai izveidotu globālus standartus, t. i., normu kopumu un atbildības mehānismus, kas nosaka veidu, kā pret cilvēkiem ir jāizturas. Cilvēktiesības nodrošina universālu obligāto standartu kopumu, kas cita starpā balstās uz cilvēka cieņas, autonomijas, vienlīdzības un tiesiskuma vērtībām. Šie standarti un ar tiem saistītie tiesiskie mehānismi valstīm rada juridiskus pienākumus ievērot, aizsargāt un īstenot cilvēktiesības. Tie arī pieprasa, lai personas, kurām viņu tiesības ir liegtas vai pārkāptas, varētu saņemt efektīvu tiesisko aizsardzību. Satversmes tiesa ir uzsvērusi, ka personas pamattiesību aizsardzība ir viens no demokrātiskas tiesiskas valsts nozīmīgākajiem pienākumiem.[638] Tas ir pilnībā attiecināms arī uz mākslīgo intelektu. Cilvēktiesību aizsardzība ir viens no būtiskākajiem valsts pienākumiem arī mākslīgā intelekta laikmetā.

Cilvēktiesības veido mākslīgā intelekta regulējuma pamatu, un tām ir primāra nozīme turpmākā starptautiskā un ES mākslīgā intelekta tiesiskā regulējuma attīstībā. Tas uzsvērts vairāku starptautisko organizāciju dokumentos, piemēram, Eiropas Padomes[639], ES[640] un UNESCO[641] mākslīgā intelekta ētikas vadlīnijās, kuras atsaucas uz starptautiskajiem cilvēktiesību dokumentiem. Arī tiesību zinātnieki ir uzsvēruši, ka cilvēktiesībām ir jābūt mākslīgā intelekta regulējuma pamatā.[642] Vadlīnijās noteiktie ētikas principi ir balstīti uz konkrētām cilvēktiesībām, to aizsardzību un veicināšanu, tostarp tiesībām uz vienlīdzību, nediskriminācijas principu, biedrošanās brīvību, tiesībām uz privāto dzīvi, ekonomiskajām, sociālajām un kultūras tiesībām, piemēram, tiesībām uz izglītību

637 Sk. AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

638 Satversmes tiesas 2012. gada 20. aprīļa spriedums lietā Nr. 2011-16-01, 9. punkts.

639 Council of Europe, CAHAI Secretariat (2020). Towards regulation of AI systems.

640 Eiropas Komisija (2020), Baltā grāmata par mākslīgo intelektu.

641 UNESCO, AHEG (2020), Outcome document: First Draft of the Recommendation on the Ethics of Artificial Intelligence.

642 Sk., piemēram, Mantelero (2020), Regulating AI within the Human Rights Framework.

un tiesībām uz veselību. Piemēram, ētikas princips "kaitējuma novēršana" prasa aizsargāt cilvēka cieņu, kā arī visas pārējās cilvēktiesības. Tajā pašā laikā CAHAI ir vērsusi uzmanību, ka daudzas no vadlīnijām konkrēti nenorāda uz nepieciešamību veicināt cilvēktiesības, kā arī nebrīdina par cilvēktiesību pārkāpumiem, ko var radīt mākslīgā intelekta sistēmu izstrāde un ieviešana, līdz ar to ir steidzami nepieciešams vērst lielāku uzmanību uz cilvēktiesību ietekmi.[643]

Cilvēktiesību regulējuma izmantošanai mākslīgā intelekta kontekstā ir daudzas priekšrocības: ir izveidotas institūcijas, judikatūra, tiek izmantota universāla valoda un cilvēktiesības ir starptautiski atzītas. Laika gaitā ir izveidota plaša starptautiska, reģionāla un nacionāla līmeņa cilvēktiesību aizsardzības sistēma. Tā sastāv no starptautiskām organizācijām, tiesām, nevalstiskām organizācijām un citām institūcijām, kurās var vērsties cilvēktiesību pārkāpuma gadījumā un izmantot tiesiskās aizsardzības līdzekļus. Cilvēktiesības pamatojas kopīgās vērtībās, kas kā juridiski saistošas tiesību normas tiek interpretētas un piemērotas konkrētās situācijās starptautiskajā, reģionālajā un nacionālajā tiesu praksē. Cilvēktiesības nodrošina universālu valodu globāliem jautājumiem. Cilvēktiesību aizsardzības institūcijas aktīvi piedalās diskusijās par mākslīgā intelekta vietu sabiedrībā kopā ar citām ieinteresētajām pusēm, kas ir tieši iesaistītas mākslīgā intelekta izstrādē un izmantošanā. Turklāt cilvēktiesības ir starptautiski atzītas un ietvertas juridiski saistošos tiesību aktos.[644]

OECD norāda, ka cilvēktiesībās balstītā pieeja mākslīgajam intelektam var palīdzēt identificēt riskus, it īpaši augstus riskus, prioritātes, neaizsargātās un mazāk aizsargātās grupas un nodrošināt tiesiskās aizsardzības līdzekļus. Cilvēktiesības var palīdzēt noteikt kaitējuma risku, piemēram, ja tiek veikts ietekmes uz cilvēktiesībām novērtējums, kas kā atsevišķs mehānisms aplūkots nodaļas turpinājumā. Cilvēktiesības kā minimālie standarti nosaka pamatprasības, kuras nedrīkst pārkāpt. Piemēram, regulējot izteiksmes brīvību sociālajos tīklos, cilvēktiesības palīdz noteikt naida runu kā sarkano līniju. Līdzīgā veidā cilvēktiesības, to skaitā cilvēka cieņa, nediskriminācijas princips, privātums un datu aizsardzība, būtu jāņem vērā, nosakot sejas atpazīšanas un citu novērošanas tehnoloģiju izmantošanas sarkanās līnijas, kas tālāk analizētas atsevišķi. Cilvēktiesības var palīdzēt noteikt neaizsargāto iedzīvotāju vai riska grupas, vai kopienas mākslīgā intelekta sistēmu izmantošanas gadījumā. Jau iepriekš tika atklāts, ka sievietes un atsevišķas etniskās grupas var būtiski vairāk skart sejas atpazīšanas tehnoloģiju izmantošana. Cilvēktiesības kā tiesību normas, kas rada pienākumus, var palīdzēt tiem, kuru tiesības tiek pārkāptas. Tās garantē personām tiesiskās

643 Council of Europe, CAHAI Secretariat (2020). Towards regulation of AI systems.

644 Access Now. (2018). Human rights in the age of artificial intelligence. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

aizsardzības līdzekļus, un tie var būt, piemēram, darbības pārtraukšana, jaunu procesu vai politikas izstrāde, atvainošanās vai naudas kompensācija.[645]

OECD ir vērsusi uzmanību, ka ir arī vairāki būtiski izaicinājumi, lai īstenotu uz cilvēktiesībām balstīto pieeju attiecībā uz mākslīgo intelektu. Cilvēktiesības ir vairāk vērstas uz valstīm, nevis privātiem dalībniekiem, tajā pašā laikā tieši privātā sektora dalībniekiem ir galvenā loma mākslīgā intelekta sistēmu izstrādē un ieviešanā. Vairāku starpvaldību iniciatīvu mērķis ir novērst plaisu starp valsts un privāto sektoru.[646] Privātie uzņēmumi var nebūt ieinteresēti aizsargāt cilvēktiesības, īpaši tad, ja tādējādi var tikt samazināta peļņa. Tomēr arvien vairāk tiek atzīts, ka cilvēktiesību aizsardzība sniedz labumu arī uzņēmumu biznesa interesēm. Vēl viens izaicinājums ir tas, ka cilvēktiesību aizsardzība ir saistīta ar jurisdikciju. Parasti prasītājam ir jāpierāda tiesiskais statuss noteiktā jurisdikcijā, un tas var nebūt efektīvi un radīt grūtības gadījumos, kad ir iesaistīti lieli starptautiski uzņēmumi un mākslīgā intelekta sistēmas, kas aptver vairākas jurisdikcijas. Vēl viens trūkums ir, ka cilvēktiesības ir labāk piemērotas, lai samazinātu būtisku kaitējumu nelielam skaitam cilvēku, nevis novērstu kaitējumu kolektīvām interesēm. Individuālā ceļā ir grūtāk apstrīdēt mākslīgā intelekta sistēmas, to skaitā novērošanas sistēmas, un to radīto ietekmi, kas apdraud cilvēktiesības un brīvības. Ir nepieciešama vienota un koordinēta rīcība, lai aizsargātu privātumu un autonomiju kā sabiedrības labumu. Pretējā gadījumā pastāv dziļš šo sistēmu konflikts ar demokrātijas, brīvības un vienlīdzības principu.[647] Arī dažas vispārējas mākslīgā intelekta regulējuma problēmas, piemēram, pārredzamība un izskaidrojamība, attiecas uz cilvēktiesību jautājumiem. Bez pārredzamības ir grūti noteikt, vai ir pārkāptas cilvēktiesības.[648]

Cilvēktiesības kā juridiski saistošs normu kopums kopā ar citiem saistītiem tiesiskiem un institucionāliem mehānismiem veido pamatu, lai nodrošinātu ētisku un uz cilvēku vērstu mākslīgā intelekta attīstību un izmantošanu. Jau tagad mākslīgā intelekta attīstībai un izmantošanai ir jāatbilst starptautiskajiem un ES cilvēktiesību dokumentiem, īpaši ECTK un Hartai, kā arī valstu nacionālajiem tiesību aktiem, īpaši konstitūcijām, kurās parasti ir iekļautas cilvēktiesību

645 OECD. (2019). Artificial Intelligence in Society. https://www.oecd.org/publications/artificial-intelligence-in-society-eedfee77-en.htm

646 Nesenie starpvaldību instrumenti, piemēram, ANO Uzņēmējdarbības un cilvēktiesību pamatprincipi, atzīmē privāto dalībnieku lomu cilvēktiesību kontekstā, tai skaitā paredzot to atbildību par cilvēktiesību ievērošanu. Sk. OHCHR. (2011). Guiding Principles on Business and Human Rights. Implementing the United Nations "Protect, Respect and Remedy" Framework. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

647 Lewandowsky, Smillie, Garcia, et al. (2020), Technology and Democracy.

648 OECD (2019), Artificial Intelligence in Society.

normas. Kā tika atklāts grāmatas otrajā nodaļā, cilvēktiesību normas jau šobrīd ir piemērojamas un paredz juridiski saistošas prasības attiecībā uz mākslīgā intelekta novērošanas sistēmām. Daudzas prasības, kas noteiktas ētikas vadlīnijās, jau ir ietvertas gan cilvēktiesību, gan citos tiesību aktos.

Eiropas cilvēktiesību aizsardzības sistēmā varētu tikt izveidots uz cilvēktiesībām balstīts mākslīgā intelekta regulējums, kas kalpotu par paraugu pārējai pasaulei. ES pamatā ir cilvēka cieņas, brīvības, demokrātijas, tiesiskuma un cilvēktiesību ievērošanas vērtības. ES varētu radīt "zelta standartu" regulas formā cilvēktiesībās balstītam mākslīgā intelekta regulējumam, kas būtu tiešā veidā piemērojama visās dalībvalstīs, līdzīgi kā ES datu aizsardzības noteikumi. Arī Eiropas Padome varētu izstrādāt skaidru uz cilvēktiesībām, tiesiskumu un demokrātiskām vērtībām balstītu regulējumu, pieņemot jaunu saistošu tiesisko instrumentu, piemēram, pamatkonvenciju.

Izstrādājot mākslīgā intelekta tiesisko regulējumu, cilvēktiesību normas būtu attīstāmas tālāk, skaidri nosakot to piemērošanu attiecībā uz konkrētiem to izmantošanas gadījumiem. Šīs grāmatas iepriekšējās nodaļās veiktā analīze atklāj, ka ir nepieciešams ierobežot un stingri regulēt valstu masveida novērošanas praksi, kas īstenota, izmantojot mākslīgā intelekta tehnoloģijas, lai tā atbilstu cilvēktiesībām, un ir nepieciešams noteikt skaidras robežas un atbildības mehānismus. Atkāpšanās no cilvēktiesībām īpašos izņēmuma apstākļos, piemēram, drošības nolūkos, būtu atļaujama, tikai ja tas ir stingri jeb absolūti nepieciešams un ievērojot ierobežošanas nosacījumus.

Pašreizējā uz cilvēktiesībām balstītā pieeja mākslīgajam intelektam ir jāpilnveido, lai izvairītos no vispārēju politikas ieteikumu noteikšanas vai tādu vispārīgu principu atkārtošanas, kuriem trūkst pienācīgas kontekstualizācijas, piemēram, nediskriminācija un pārredzamība, tas ir izšķiroši jebkuram normatīvajam regulējumam. Tādējādi turpmākajam mākslīgā intelekta regulējumam jābūt balstītam uz esošajiem cilvēktiesību instrumentiem, bet šim regulējumam vajadzētu arī spēt pielāgot un kontekstualizēt šo tiesību piemērošanu un novērst trūkumus, ko rada tiesību akti, kas izstrādāti pirms mākslīgā intelekta laikmeta.[649]

Kā tika atklāts iepriekš, mākslīgā intelekta sistēmu izmantošana var būtiski aizskart cilvēktiesības, īpaši tiesības uz privātumu un datu aizsardzību, radīt aizspriedumus un diskrimināciju. Līdzās cilvēktiesību riskiem šīm tehnoloģijām ir plašāka ietekme uz tiesiskumu un demokrātiju, un to ir grūti paredzēt vai izmērīt.

Vācijas tiesību zinātnieks Pauls Nemics (*Paul Nemitz*) norāda, ka cilvēktiesības, demokrātija un tiesiskums ir Rietumu liberālo konstitūciju pamatelementi, mūsu konstitucionālās ticības "trinitārā formula". Šie principi ir augstākais likums – visas valdības, likumdevēju un sabiedrībā notiekošie procesi tiek vērtēti,

649 Mantelero (2020), Regulating AI within the Human Rights Framework, p. 480.

vadoties no tiem. Ņemot vērā mākslīgā intelekta paredzamo straujo izplatību mūsdienu sabiedrībā, ir nepieciešams uzdot jautājumu, kā šīs jaunās tehnoloģijas veidot tā, lai atbalstītu konstitucionālo "trinitāro formulu" un to nostiprinātu, nevis vājinātu. Šeit piedāvātā atbilde – mums ir nepieciešama jauna tehnoloģiju un biznesa attīstības kultūra mākslīgā intelekta laikmetam, kas integrē tiesiskumu, demokrātiju un cilvēktiesības.[650] Atrast veidus, kā jaunās tehnoloģijas attīstīt un ieviest tikai tā, lai aizsargātu cilvēka brīvību un cieņu, kā arī konstitucionālās demokrātijas pamatus, proti, demokrātiju, tiesiskumu un cilvēktiesības, ir mūsu laika izaicinājums.[651] Lai arī pašreizējais Eiropas cilvēktiesību, privātuma un datu aizsardzības regulējums ir būtisks, tas nav pietiekams, lai novērstu visus riskus, ko rada mākslīgais intelekts. Jaunie izaicinājumi prasa jauna regulējuma izstrādi globālā līmenī, Eiropas – ES un Eiropas Padomes – līmenī, kā arī nacionālā līmenī.

7.3. Jauna mākslīgā intelekta tiesiskā regulējuma nepieciešamība

Jauna mākslīgā intelekta regulējuma izstrādi pamato nepieciešamība novērst iespējamo kaitējumu, ko mākslīgā intelekta sistēmu izmantošana var radīt. Brūss Šneiers salīdzina jauno tehnoloģiju attīstību ar lidmašīnu ieviešanu. Mūsdienās, kad kāpjam lidmašīnā, mēs pamatā jūtamies droši, ka lidojums beigsies labi, bet sākumā lidmašīnas nebija drošs pārvietošanās līdzeklis, un ar tām lidot bija bīstami. 1972. gadā avarēja 72 lidmašīnas un bojā gāja vairāk nekā 2000 cilvēku. Tas, kas mainījās, bija lidmašīnu drošības regulējums. Pagāja gadu desmiti, valdības noteica dažāda veida uzlabojumus lidmašīnu dizainam, lidojumu procedūrām, pilotu apmācībām utt. Tagad lidmašīnas ir drošs veids ceļošanai.[652]

Līdzīgā veidā mēs mūsdienās arvien skaidrāk redzam, kādu kaitējumu var radīt jaunās tehnoloģijas un mākslīgais intelekts, un arvien vairāk apzināmies nepieciešamību izveidot stingru regulējumu, kas to novērstu. Tajā pašā laikā jaunās tehnoloģijas atšķirībā no lidmašīnām var izmantot ļoti dažādos un pat grūti prognozējamos veidos, kā arī dažādās jomās, un tas apgrūtina skaidra regulējuma izveidi, turklāt prasa komplicētu pieeju, apvienojot dažādus regulējuma veidus.

650 Nemitz, P. (2018). Constitutional Democracy and Technology in the Age of Artificial Intelligence. *Philos. Trans. R. Soc. A-Math. Phys. Eng. Sci.,* 376(2133). https://doi.org/10.1098/RSTA.2018.0089

651 Nemitz, P. (2018). Profiling the European Citizen: Why today's democracy needs to look harder at the negative potential of new technology than at its positive potential. In: Bayamlioğlu, E., Baraliuc, I., Janssens, L. u. a. (eds.), *Being Profiled: Cogitas Ergo Sum. 10 Years of Profiling the European Citizen.* Amsterdam: Amsterdam University Press, pp. 8–11. https://doi.org/10.2307/j.ctvhrd092.3

652 Sk. Schneier (2016), *Data and Goliath* .., p. 144.

Tiesiskajam regulējumam ir vairāki trūkumi. Viens no lielākajiem izaicinājumiem – tehnoloģijas attīstās daudz ātrāk, nekā tiek pieņemti jauni likumi. Tiesību aktu pieņemšanas process ir ilgs, tāpēc tas netiek līdzi straujajai tehnoloģiju attīstībai. Tiesību normas to pieņemšanas brīdī bieži vien jau vairs neatbilst esošajām jaunākajām tehnoloģiju attīstības tendencēm. Līdzīgi arī esošie tiesiskie instrumenti, kas pieņemti pirms mākslīgā intelekta sistēmu plašas izmantošanas, mēdz mazināt to efektivitāti un neļauj adekvāti un konkrēti reaģēt uz mākslīgā intelekta sistēmu izaicinājumiem, jo nav pielāgoti to specifikai.[653]

Vēl viens arguments, ko bieži izmanto privātie uzņēmumi, iebilstot pret jaunām tiesiskām prasībām, – tiesiskais regulējums var kavēt inovāciju un tehnoloģiju attīstību. Daudzos gadījumos tiesiskais regulējums var nebūt piemērotākais līdzeklis. Pastāv arī citi rīcības veidi, kas konkrētu tehnoloģiju regulēšanai var būt piemērotāki salīdzinājumā ar juridiski saistošiem noteikumiem. Piemēram, ētikas noteikumi vai sertifikācija var definēt un palīdzēt īstenot prasības jauno tehnoloģiju izstrādei un izmantošanai, kā arī var palīdzēt panākt, lai sabiedrība tām uzticas. Tomēr pašregulācija nav pietiekama. Tā nevar efektīvi darboties gadījumā, kad tehnoloģiju izmantošana var radīt kaitējumu. Būtu naivi cerēt, ka uzņēmumi, kas gūst peļņu no tehnoloģiju izstrādes un izmantošanas, paši tās regulēs un ierobežos to izmantošanu. Regulējumam ir jābūt samērīgam, proporcionālam, elastīgam, lai veicinātu inovāciju un tehnoloģiju attīstību un sabiedrības uzticību. Savukārt stingrs tiesiskais regulējums, kas nosaka ierobežojumus un sankcijas, būtu jāizmanto gadījumos, kad jaunās tehnoloģijas var radīt kaitējumu cilvēkiem, viņu tiesībām, drošībai, sabiedrības vērtībām un demokrātijai, kā arī var radīt cita veida būtisku kaitējumu, lai panāktu, ka tas tiek novērsts.

Eiropas Padome vērš uzmanību – lai gan attiecībā uz mākslīgo intelektu nepastāv tiesiskais vakuums, tomēr eksistē tiesiskas nepilnības. Pirmkārt, tiesības un pienākumi, kas minēti spēkā esošajos tiesiskajos instrumentos, īpaši cilvēktiesību normās, parasti tiek formulēti plaši vai vispārīgi. Tas pats par sevi nav problemātiski, tomēr dažos gadījumos var būt grūtības tos interpretēt attiecībā uz mākslīgā intelekta sistēmām. Turklāt tie nepārprotami nerisina dažus ar mākslīgo intelektu saistītus jautājumus, tādējādi traucējot to efektīvu piemērošanu situācijās, ko rada mākslīgā intelekta sistēmas. Otrkārt, vairāki būtiski principi, kas attiecas uz cilvēktiesību, demokrātijas un tiesiskuma aizsardzību mākslīgā intelekta jomā, pašlaik nav tieši tiesiski noteikti. Šīs nepilnības attiecas, piemēram, uz nepieciešamību nodrošināt pietiekamu cilvēku kontroli un uzraudzību, sistēmu tehnisko noturību, efektīvu pārredzamību un izskaidrojamību, it īpaši, ja mākslīgā intelekta sistēmu izmantošana rada tiesiskas vai citas būtiskas sekas

653 Council of Europe, CAHAI (2020), Feasibility Study.

personām. Treškārt, pašreizējie instrumenti arī nepievērš pietiekamu uzmanību pasākumiem, kas jāveic sistēmu izstrādātājiem un lietotājiem, lai nodrošinātu šo sistēmu efektivitāti ikreiz, kad tās var ietekmēt cilvēktiesības, demokrātiju vai tiesiskumu, un nodrošinātu, ka tiem ir nepieciešamā kompetence vai profesionālā kvalifikācija. Šīs juridiskās nepilnības un paredzama un pamatota tiesiskā regulējuma trūkums var radīt nenoteiktību mākslīgā intelekta izstrādātājiem, piegādātājiem un lietotājiem.[654]

Arvien vairāk tiek atzīts, ka ir nepieciešams skaidrs mākslīgā intelekta tiesiskais regulējums. Kā jau tika atklāts iepriekš, Eiropas Komisija ir publicējusi MI akta priekšlikumu.[655] Arī Eiropas Padome šobrīd apsver jauna mākslīgā intelekta tiesiskā regulējuma izstrādi, kas varētu apvienot jauna saistoša tiesiskā instrumenta, piemēram, konvencijas vai pamatkonvencijas, pieņemšanu, nesaistošus tiesiskos instrumentus, kā arī nozaru jeb sektorālā tiesiskā regulējuma pilnveidošanu.[656]

Viena no jomām, kas būtu īpaši regulējama, ir automatizēto lēmumu pieņemšana, tostarp izmantojot novērošanas tehnoloģijas. Džovanni Sartors secina, ka attiecībā uz mākslīgā intelekta sistēmu izmantošanu var tikt ievēroti datu aizsardzības noteikumi un nav nepieciešamas būtiskas izmaiņas esošā datu aizsardzības regulējumā.[657] Tajā pašā laikā var tikt apgrūtināta dažu prasību īstenošana. Tāpēc būtu skaidrāk jānosaka, kā datu aizsardzības prasības, piemēram, pārredzamības prasības un prasības, kas attiecas uz automatizētu lēmumu pieņemšanu, ir piemērojamas konkrētos gadījumos.[658]

Tiesību jomas eksperti iesaka stiprināt esošās cilvēktiesības, kā arī apsvērt iespējas regulējumā noteikt pielāgotas vai pat jauna veida cilvēktiesības. Piemēram, AI HLEG dalībniece Kateleine Millere (*Catelijne Muller*) norāda, ka būtu apsveramas vairākas pielāgotas vai pat jaunas cilvēktiesības: tiesības uz cilvēka autonomiju; cilvēka uzraudzība pār mākslīgo intelektu; atsevišķas tiesības uz fizisko, psiholoģisko un morālo integritāti, ņemot vērā mākslīgā intelekta profilēšanu un emociju atpazīšanu. Tiek ieteikts arī stiprināt un pielāgot tiesības uz privātumu, lai aizsargātu pret mākslīgā intelekta masveida novērošanu un nediferencētu, sabiedrības mēroga personu novērošanu tiešsaistē, izmantojot gan personas datus, gan nepersondatus.[659] Esošās cilvēktiesību normas jau šobrīd

654 Council of Europe, CAHAI (2020), Feasibility Study.

655 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

656 Council of Europe, CAHAI (2020), Feasibility Study.

657 Sartor, Lagioia (2020), The Impact of the General Data Protection Regulation ..

658 Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence.

659 Ibid.

ietver daudzus no minētajiem aspektiem. Šīs normas būtu pielāgojamas un konkretizējamas nākotnes mākslīgā intelekta tiesiskajā regulējumā.

Cilvēktiesību un datu aizsardzības regulējumu vajadzētu vairāk attiecināt uz kolektīvo interešu aizsardzību, uz ko ir vērsuši uzmanību daudzi tiesību zinātnieki.[660] Kā tika atklāts grāmatas 3.6. nodaļā, datu aizsardzības eksperti ir pierādījuši, ka lielo datu analītikas attīstība prasa jaunu grupu privātuma aizsardzību, veltot īpašu uzmanību algoritmiskās klasifikācijas rezultātā veidotajām grupām.[661]

Mākslīgā intelekta tiesiskais regulējums pēc iespējas ir jāpielāgo konkrētās jomas specifikai, it īpaši augsta riska jomās, tostarp tiesībaizsardzībā. Ņemot vērā, ka cilvēktiesību un datu aizsardzības tiesību akti, īpaši VDAR un Policijas direktīva, paredz svarīgas prasības attiecībā uz mākslīgā intelekta novērošanas tehnoloģiju ieviešanu un izmantošanu, būtu nepieciešams konkretizēt, kā tās ir piemērojamas attiecībā uz valsts novērošanas pasākumiem. Eiropas Padome sevišķi uzsver nepieciešamību regulēt sejas atpazīšanas tehnoloģijas. Vadlīnijas par sejas atpazīšanu mudina valstis izstrādāt un pieņemt specifiskus noteikumus, kas regulētu sejas atpazīšanas tehnoloģiju biometrisko apstrādi, kura tiek veikta tiesībaizsardzības nolūkos.[662]

Kā tika atklāts grāmatā, kaut gan esošais regulējums paredz būtiskas prasības, pašreiz spēkā esošais tiesiskais regulējums nav pietiekams, lai tiktu galā ar mākslīgā intelekta novērošanas tehnoloģiju radīto apdraudējumu. Lai novērstu šos izaicinājumus, būtiska nozīme ir arī skaidru ierobežojumu jeb sarkano līniju noteikšanai.

7.4. Sarkano līniju noteikšana

Skaidru sarkano līniju noteikšanai ir ļoti svarīga nozīme, lai novērstu tādu mākslīgā intelekta sistēmu izmantošanu, kas pārkāpj cilvēktiesības. Tiesiski noteiktiem ierobežojumiem ir jābūt neatņemamai uz cilvēktiesībām balstīta mākslīgā intelekta tiesiskā regulējuma sastāvdaļai. Gan zinātnieki, gan pilsoniskās sabiedrības organizāciju pārstāvji arvien vairāk mudina noteikt skaidrus normatīvus ierobežojumus tāda mākslīgā intelekta izmantošanai, kas ir pretrunā cilvēktiesībām.

660 Mantelero, A. (2017). Regulating Big Data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer Law & Security Review,* 33, pp. 584–602.

661 Sk., piemēram, Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. *Philosophy & Technology*, 30(4), pp. 475–494. https://doi.org/10.1007/s13347-017-0253-7

662 Council of Europe (2021), .. Convention 108.

Turīnas Politehniskās universitātes tiesību zinātnieks, datu ētikas un datu aizsardzības eksperts asociētais profesors Alesandro Mantelero vērš uzmanību, ka cilvēka cieņai un cilvēktiesībām ir centrālā nozīme mākslīgā intelekta izmantošanā. Viņš rosina ieviest aizliegumus konkrētām mākslīgā intelekta tehnoloģijām, kuras tiek izstrādātas veidā, kas ir pretrunā ar cilvēktiesībām, demokrātiju un tiesiskumu.[663]

Oksfordas Universitātes asociētā profesore Karisa Velisa grāmatā "Privātums ir vara" (*Privacy is Power* – angļu val.) mudina stingri ierobežot valsts novērošanu, norādot, ka valsts iestādēm nav jāveic masveida novērošana, lai iedzīvotāji būtu drošībā. Datu vākšana un analīze nedrīkstētu notikt bez ordera, un tā var notikt tikai nepieciešamības gadījumā. Tai ir jābūt mērķtiecīgai, pretstatā masveida novērošanai, kā arī proporcionālai. Zinātniece uzskata, ka dažas no novērošanas tehnoloģijām ir tik bīstamas un tik piemērotas ļaunprātīgai izmantošanai, ka būtu labāk tās aizliegt visas kopā, tāpat kā mēs aizliedzam dažus ieročus. Mums vajadzētu apsvērt iespēju aizliegt sejas atpazīšanu, kā arī gaitas un sirdspukstu atpazīšanu un citas tehnoloģijas, kas iznīcina anonimitāti, jo tie ir ideāli instrumenti apspiešanai.[664]

Arvien skaļāk normatīvi noteikt mākslīgā intelekta izmantošanas sarkanās līnijas pieprasa arī cilvēktiesību aizstāvības organizācijas. 2021. gada 21. janvārī EDRi kopā ar 60 pilsoniskās sabiedrības organizācijām iesniedza Eiropas Komisijai atklātu vēstuli, kurā aicina ieviest sarkanās līnijas gaidāmajā mākslīgā intelekta regulējuma priekšlikumā.[665] Tās aicina noteikt normatīvos ierobežojumus tāda mākslīgā intelekta izmantošanai, kas nepamatoti ierobežo cilvēktiesības. Vēstulē norādīts, ka papildus VDAR stingrai ievērošanai un tādiem aizsardzības pasākumiem kā ietekmes uz cilvēktiesībām novērtējums, programmatūras pārredzamība un datu kopuma pieejamība publiskai pārbaudei, ir svarīgi, lai topošajā tiesību akta priekšlikumā tiktu noteikti skaidri ierobežojumi, kas nosaka, ko var un ko nevar uzskatīt par likumīgu mākslīgā intelekta izmantošanu, lai nepārprotami risinātu vairākus jautājumus. Tie ir: biometriskā masveida novērošana un publisko vietu uzraudzība; strukturālā diskriminācija, atstumtība un kolektīvā kaitējuma saasināšana; tādu svarīgu pakalpojumu kā veselības aprūpe un sociālie pakalpojumi ierobežošana un diskriminējoša piekļuve; darbinieku novērošana un darba ņēmēju pamattiesību pārkāpumi; taisnīgas tiesas un procesuālo tiesību

663 Mantelero (2020), Regulating AI within the Human Rights Framework, p. 501; sk. arī Kindt, E. (2020). A First Attempt at Regulating Biomentric Data in the European Union, p. 68. In: Kak, A. (ed.). *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute, pp. 62–68. https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions

664 Véliz (2021), *Privacy Is Power*, pp. 152, 154.

665 EDRi (12 January, 2021), Re: Open letter: Civil society call for the introduction of red lines ..

pieejamības apgrūtināšana; tādu sistēmu izmantošana, kas izdara secinājumus un prognozes par mūsu vissensitīvākajām īpašībām, uzvedību un domām; īpaši būtiski – manipulācijas ar cilvēku uzvedību vai tās kontrole un ar to saistītie cilvēka cieņas, rīcības brīvības un kolektīvās demokrātijas apdraudējumi.

Vēstulē tiek mudināts it īpaši pievērst uzmanību konkrētiem mākslīgā intelekta izmantošanas veidiem, kas nav saderīgi ar demokrātisku sabiedrību un kas ir jāaizliedz vai jāierobežo mākslīgā intelekta tiesiskajā regulējumā. Pirmkārt, mākslīgā intelekta tiesību akta priekšlikumā būtu jāiekļauj nepārprotams aizliegums biometrisko datu izmantošanai bez izšķirības vai patvaļīgai mērķtiecīgai izmantošanai publiskās vai publiski pieejamās vietās, kas var izraisīt masveida novērošanu. Tas nodrošinātu, ka tiesībaizsardzības un citas valsts iestādes, kā arī privātas iestādes un uzņēmumi nevarētu ļaunprātīgi izmantot plašos izņēmumus un rīcības brīvību, kas pašlaik ir iespējama saskaņā ar vispārējiem principiem, kas nosaka biometriskās apstrādes aizliegumu. Otrkārt, Eiropas Komisija tiek mudināta tiesiskajā regulējumā noteikt ierobežojumus attiecībā uz izmantošanas veidiem, kas ir pretrunā pamattiesībām, ieskaitot mākslīgā intelekta izmantošanu robežkontrolē, prognozēšanā tiesībaizsardzības nolūkos, arī uz sistēmām, kas ierobežo piekļuvi sociālajām tiesībām un pabalstiem, un riska novērtēšanas rīkiem krimināltiesību kontekstā. Treškārt, turpmākā mākslīgā intelekta tiesību aktu un politikas izstrādē ir jāiekļauj marginalizētās un aizskartās kopienas.

EDRi pieteiktajā ES pilsoņu iniciatīvā "Atgūsti savu seju" pilsoniskās sabiedrības organizācijas pieprasa Eiropas Komisiju tiesību aktos un praksē aizliegt biometrisko masveida novērošanu. Masveida biometriskās apstrādes sistēmas nedrīkst izstrādāt, ieviest pat izmēģinājuma veidā vai izmantot publiskas vai privātas iestādes, ciktāl tās var radīt nevajadzīgu vai nesamērīgu iejaukšanos cilvēku pamattiesībās. Pierādījumi liecina, ka biometriskās masveida novērošanas izmantošana dalībvalstīs un ES aģentūrās ir izraisījusi ES datu aizsardzības tiesību pārkāpumus un nepamatoti ierobežojusi cilvēktiesības, tostarp tiesības uz privātumu, vārda brīvību, tiesības protestēt un netikt diskriminētam. Biometriskās uzraudzības, profilēšanas un prognozēšanas plaša izmantošana apdraud tiesiskumu un cilvēka pamatbrīvības. Tāpēc Eiropas Komisija tiek mudināta sagatavot tiesību aktu, kas skaidri aizliegtu biometrisko masveida novērošanu un tādējādi atbilstu spēkā esošajām ES datu aizsardzības prasībām.[666]

Nepieciešamību noteikt mākslīgā intelekta izmantošanas sarkanās līnijas ir uzsvērušas arī starptautiskās organizācijas. UNESCO Rekomendācija par mākslīgā intelekta ētiku paredz, ka mākslīgā intelekta sistēmas nedrīkst izmantot sociālai novērtēšanai vai masveida novērošanai (26. punkts).[667]

666 EDRi (17 February, 2021), New ECI calls Europeans to stand ..; European Citizens' Initiative ..

667 UNESCO (2021), Recommendation on the Ethics of Artificial Intelligence.

CAHAI 2020. gada decembra pētījumā norādīts, ka sarkanās līnijas varētu noteikt tādu mākslīgā intelekta sistēmu izmantošanai, kas tiek uzskatītas par pārāk ietekmīgām, lai tās atstātu nekontrolētas vai neregulētas, vai pat – atļautu. Var būt nepieciešams noteikt aizliegumu, pagaidu aizliegumu, stingrus ierobežojumus vai nosacījumus ārkārtas vai arī kontrolētai šādu mākslīgā intelekta sistēmu izmantošanai: sejas atpazīšanas un citu biometrisko atpazīšanas veidu izmantošanai bez izšķirības valsts vai privātajā sektorā; uz mākslīgo intelektu balstītai masveida novērošanai (izmantojot sejas, biometrisko atpazīšanu, kā arī citus mākslīgā intelekta vai identifikācijas veidus, piemēram, atrašanās vietas noteikšanas pakalpojumus, uzvedības novērošanu tiešsaistē utt.); personiskai, fiziskai vai garīgai analizēšanai, novērtēšanai, profilēšanai un uzvedības virzīšanai, izmantojot biometrisko un uzvedības atpazīšanu; sociālajai novērtēšanai ar mākslīgā intelekta palīdzību; slēptām mākslīgā intelekta sistēmām un dziļviltojumu tehnoloģijām (*deep fakes* – angļu val.); cilvēka un mākslīgā intelekta saskarnēm (*human-AI interfaces* – angļu val.).[668]

2020. gada decembrī Eiropas Padomes publicētajā CAHAI priekšizpētes ziņojumā tāpat ir norādīts, ka starptautiska nolīguma izveide par apšaubāma mākslīgā intelekta izmantošanu un sarkanajām līnijām var būt būtiska. Lietojumprogrammas, uz kurām varētu attiecināt sarkanās līnijas, ir, piemēram: attālinātas biometriskās atpazīšanas sistēmas vai citas uz mākslīgo intelektu balstītas novērošanas lietojumprogrammas, kas var izraisīt masveida novērošanu vai sociālo vērtēšanu; mākslīgā intelekta izmantošana slēptai manipulācijai ar personām. Katrs no šiem veidiem būtiski ietekmē personas autonomiju, kā arī demokrātijas pamatprincipus un brīvības. Šādu tehnoloģiju izmantošana, piemēram, valsts drošības mērķiem, būtu īpaši jāparedz ar likumu, tai ir jābūt nepieciešamai demokrātiskā sabiedrībā un proporcionālai likumīgam mērķim, un pieļaujamai tikai kontrolētā vidē un ierobežotu laika periodu.[669]

Eiropas Padomes sejas atpazīšanas vadlīnijās ir vērsta uzmanība, ka biometrisko datu apstrāde ar sejas atpazīšanas tehnoloģiju identifikācijas nolūkā būtu jāatļauj tikai saistībā ar tiesībaizsardzības mērķiem, ievērojot stingras nepieciešamības un samērīguma principus. Vadlīnijās valstu likumdevēji tiek mudināti pieņemt speciālus noteikumus attiecībā uz sejas atpazīšanas tehnoloģiju biometrisko apstrādi, citiem mērķiem nosakot precīzus izmantošanas pamatus, kā arī tajās vērsta uzmanība, ka privātie uzņēmumi nedrīkst izmantot sejas atpazīšanas tehnoloģijas nekontrolētā vidē, piemēram, iepirkšanās centros. Vienlaikus minētās vadlīnijas nenosaka skaidrus ierobežojumus vai pagaidu aizlieguma

668 Council of Europe, CAHAI Secretariat (2020), Towards regulation of AI systems; sk. arī Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence.

669 Council of Europe, CAHAI (2020), Feasibility Study.

piemērošanu attiecībā uz sejas atpazīšanas tehnoloģiju izmantošanu, ko veic tiesībaizsardzības vai citas valsts iestādes.[670]

Eiropas Savienībā arī ir vērsta uzmanība uz nepieciešamību noteikt sarkanās līnijas mākslīgā intelekta sistēmu izmantošanai. 2020. gada jūnijā Eiropas Parlamenta Pilsoņu brīvību, tieslietu un iekšlietu komiteja (LIBE) publicēja viedokli, kurā aicināja Eiropas Komisiju novērtēt pagaidu aizlieguma sekas sejas atpazīšanas sistēmu izmantošanā un atkarībā no šāda novērtējuma rezultātiem apsvērt pagaidu aizliegumu šo sistēmu izmantošanai valsts iestādēm publiskās vietās, izglītībā un veselības aprūpē, kā arī tiesībaizsardzības iestādēm daļēji publiskās vietās, piemēram, lidostās, līdz tehniskos standartus varēs uzskatīt par pilnībā atbilstošiem pamattiesībām, iegūtie rezultāti būs bez aizspriedumiem un nediskriminējoši un pastāvēs stingri drošības pasākumi pret ļaunprātīgu izmantošanu, un tie nodrošinās šādu tehnoloģiju izmantošanas nepieciešamību un proporcionalitāti.[671]

Eiropas Parlamenta 2020. gada 20. oktobrī mākslīgā intelekta tiesiskā regulējuma priekšlikumā netika noteiktas skaidras sarkanās līnijas. Tas neparedzēja aizliegumu mākslīgā intelekta masveida novērošanas tehnoloģiju izmantošanai, bet pamatā balstījās uz riska novērtējumu, nosakot pienākumus attiecībā uz augsta riska tehnoloģijām. Vienlaikus Eiropas Parlamenta rezolūcijā tiek uzsvērts: "Kaut gan mākslīgā intelekta, robotikas un saistīto tehnoloģiju ieviešanai publiskā sektora lēmumu pieņemšanā ir savas priekšrocības, no tās var rasties nepareizas lietošanas prakse ar smagām sekām, piemēram, masveida novērošana, prognozēšana tiesībaizsardzības nolūkā un attiecīgu procesuālo tiesību pārkāpumi."[672] Tātad masveida novērošana un prognozēšana tiesībaizsardzības nolūkā tiek uzskatīta par mākslīgā intelekta izmantošanu, kas rada "smagas sekas". Tāpat Eiropas Parlaments vērš uzmanību, ka pret tehnoloģijām, ko var izmantot automatizētu lēmumu pieņemšanai, tādējādi aizstājot publisko iestāžu pieņemtus lēmumus, ir jāizturas ar vislielāko piesardzību, it īpaši tiesas spriešanā un tiesībaizsardzībā. Dalībvalstīm šādas tehnoloģijas būtu jāizmanto tikai tad, ja ir pārliecinoši pierādījumi par to uzticamību un gadījumos, kad var tikt apdraudētas pamatbrīvības, ir iespējama vai sistemātiski tiek veikta jēgpilna cilvēka iejaukšanās un pārskatīšana. Tiek uzsvērts, ka svarīgi ir, lai valsts iestādes šajos gadījumos veic rūpīgu mākslīgā intelekta sistēmu pamattiesību ietekmes novērtējumu,

670 Council of Europe (2021), .. Convention 108.

671 European Parliament. Committee on Civil Liberties, Justice and Home Affairs (LIBE). (2020). Draft Report on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)), LIBE, Rapporteur Tudor Ciuhodaru. https://www.europarl.europa.eu/doceo/document/LIBE-PR-652625_EN.pdf

672 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

it īpaši tad, ja tās rada augstu risku. Ietekmes novērtējums kā atsevišķs mehānisms apskatīts nodaļas turpinājumā.[673]

Eiropas Komisijas MI akta priekšlikums savukārt paredz vairākas sarkanās līnijas. Aizliegumi ietver praksi, kurai var būt ievērojams potenciāls manipulēt ar personām, izmantojot subliminālus paņēmienus, personām to neapzinoties, vai izmantojot kādu neaizsargātu grupu, piemēram, bērnu vai invalīdu, ietekmējamību ar mērķi būtiski iespaidot viņu uzvedību veidā, kas var nodarīt fizisku vai psiholoģisku kaitējumu viņiem vai kādai citai personai. Priekšlikums arī aizliedz uz mākslīgo intelektu balstītu sociālo novērtēšanu, ko vispārējiem mērķiem veic publiskā sektora iestādes. Visbeidzot, aizliegta ir arī reāllaika biometriskās tālidentifikācijas sistēmu izmantošana sabiedriskās vietās tiesībaizsardzības nolūkos, ja vien nav piemērojami kādi ierobežoti izņēmumi.[674] Kā minēts ceturtajā nodaļā, minētajiem noteikumiem tika veltīta plaša kritika. Eiropas Datu aizsardzības uzraudzītājs un Eiropas Datu aizsardzības kolēģija kopīgajā viedoklī vērš uzmanību, ka sarkanās līnijas būtu jānosaka daudz stingrāk, un aicina vispārīgi aizliegt mākslīgā intelekta izmantošanu, lai automātiski noteiktu cilvēka pazīmes sabiedriskās vietās, piemēram, ne tikai no sejas attēla, bet arī no gaitas, pirkstu nospiedumiem, DNS, balss un citiem biometriskiem vai uzvedības signāliem jebkurā kontekstā. Minētās iestādes arī iesaka aizliegt kategorizēt personas, izmantojot biometriskos datus, pēc etniskās piederības, dzimuma, kā arī politiskās vai seksuālās orientācijas vai citiem diskriminācijas pamatiem. Tās vērš uzmanību, ka mākslīgā intelekta izmantošana fiziskas personas emociju uztveršanai ir ļoti nevēlama un tā būtu jāaizliedz. Iestādes arī norāda, ka būtu aizliedzamas mākslīgā intelekta sistēmas, kas nosaka vai klasificē personas turpmāko uzvedību, ņemot vērā, ka tās aizskar cilvēka cieņas būtību. Proti, tiesībaizsardzības iestādēm būtu aizliedzams izmantot mākslīgā intelekta sistēmas, lai veiktu individuālus riska novērtējumus, kuros vērtē: risku, ka fiziska persona izdarīs pārkāpumu vai atkārtotu pārkāpumu, vai risku, kam pakļauti iespējamie noziedzīgos nodarījumos cietušie. Tāpat būtu aizliedzamas mākslīgā intelekta sistēmas, ko paredzēts izmantot izdarīta vai paredzama noziedzīga nodarījuma izdarīšanas vai tā atkārtošanas prognozēšanai, pamatojoties uz fizisku personu profilēšanu, vai fizisku personu vai grupu personības un rakstura īpašību vai agrākas noziedzīgas rīcības novērtēšanai.[675]

Kā tika atklāts pirmajā nodaļā, vairākas ASV pilsētas ir jau noteikušas sarkanās līnijas sejas atpazīšanas tehnoloģiju izmantošanai tiesībaizsardzības iestādēs. Līdzīgi kā ES, arī ASV vairāk nekā 40 pilsoniskās sabiedrības organizācijas vēstulē

673 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

674 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

675 EDPB, EDPS (2021), EDPB-EDPS Joint Opinion 5/2021 ..

ASV prezidentam Džo Baidenam (*Joseph Robinette Biden*) aicina federālā līmenī steidzami noteikt pagaidu aizliegumu sejas atpazīšanas tehnoloģiju izmantošanai.[676] 2020. gada 2. decembrī Eiropas Komisija ierosināja jaunu ES un ASV globālo pārmaiņu programmu, kas aptver plašu tēmu loku, kurā tā aicina sākt kopā rīkoties attiecībā uz mākslīgo intelektu – balstoties uz kopīgo pārliecību par pieeju, kas būtu orientēta uz cilvēkiem, un risinot tādus jautājumus kā sejas atpazīšana –, kā arī vērš uzmanību, ka ES ierosinās sākt darbu pie transatlantiskā mākslīgā intelekta nolīguma, lai izveidotu vērtībām atbilstošu reģionālo un globālo standartu plānu.[677]

Starptautiskā, Eiropas, kā arī nacionālā līmenī būtu svarīgi stingri iestāties par cilvēktiesību ievērošanu un noteikt skaidras sarkanās līnijas. Būtu jāaizliedz mākslīgā intelekta novērošanas tehnoloģiju, it īpaši sejas atpazīšanas tehnoloģiju, izmantošana masveida novērošanai. Tiesiskajā regulējumā būtu jāparedz pagaidu aizliegums tiesībaizsardzības iestādēm izmantot sejas atpazīšanas tehnoloģijas, cita starpā mērķtiecīgai novērošanai, kamēr nepastāv skaidri pierādījumi par to efektivitāti, nav pieņemts atbilstošs regulējums, nosakot to ierobežojumus un aizsardzības pasākumus, un izstrādāti noteikti kritēriji, pēc kuriem var izvērtēt to darbības likumību un atbilstību cilvēktiesību prasībām. Būtu jāaizliedz arī personu emociju uztveršanas sistēmu, kā arī biometriskās kategorizācijas sistēmu izmantošana, ņemot vērā, ka šādi mākslīgā intelekta prakses veidi pārkāpj cilvēka cieņas un autonomijas principus. Līdzīgi cilvēka cieņa tiek aizskarta, izmantojot mākslīgā intelekta sistēmas prognozēšanai tiesībaizsardzības nolūkos, kā arī migrācijas, patvēruma, robežkontroles pārvaldībā, lai noteiktu un klasificētu personas uzvedību, izmantojot personu profilēšanu vai personības un rakstura īpašību novērtēšanu. Būtu jāaizliedz arī mākslīgā intelekta sistēmu izmantošana sociālai novērtēšanai un manipulēšanai ar iedzīvotāju uzvedību. Minētie mākslīgā intelekta izmantošanas veidi rada būtisku apdraudējumu un pārkāpj cilvēka cieņu, privātumu un citas cilvēktiesības, kā arī ir pretrunā ar demokrātiskām vērtībām.

Svarīgi ir nepalaist garām izšķirošu brīdi, kad tiek aktīvi lemts par mākslīgā intelekta tiesiskā regulējuma izstrādi un kad pastāv iespēja skaidri noteikt, tostarp Eiropas Padomes un ES līmenī, vai mākslīgā intelekta sistēmu konkrēta izmantošana, kas būtiski apdraud cilvēktiesības, ir pieļaujama vai nē. Runa pat nav par to, vai mēs varētu atbalstīt konkrēto izmantošanu vai nē. Skaidri ierobežojumi,

676 Coalition Letter Requests Federal Moratorium on the Use of Facial Recognition Technology. (16 February, 2021). *Freedom House.* https://freedomhouse.org/article/coalition-letter-requests-federal-moratorium-use-facial-recognition-technology

677 European Commission. (2020). Joint Communication to the European Parliament, the European Council and the Council. A new EU-US agenda for global change. https://ec.europa.eu/info/sites/default/files/joint-communication-eu-us-agenda_en.pdf

izmantošanas aizliegumi vai pagaidu aizliegumi nemaz nav jaunu sarkano līniju noteikšana, bet jau pastāvošo atzīšana. Proti, ir jāatzīst, ka mākslīgā intelekta tehnoloģiju izmantošana masveida novērošanai jau tagad nav savietojama ar cilvēktiesībām, tiesiskumu un demokrātijas principiem.

7.5. Ietekmes novērtējums

Ietekmes novērtējums ir viens no galvenajiem mehānismiem, kura nepieciešamība ir uzsvērta gan Eiropas, gan starptautiskajos mākslīgā intelekta regulējuma priekšlikumos.[678] Līdzās ietekmei uz cilvēktiesībām mākslīgā intelekta tehnoloģijas var radīt arī plašākus riskus, kas arī būtu jāņem vērā, veicot izvērtējumu.

Alesandro Mantelero piedāvā mākslīgā intelekta cilvēktiesību, sociālās un ētiskās ietekmes novērtējuma ideju. Viņš ierosina papildus cilvēktiesībām ņemt vērā arī ētisko un sociālo ietekmi.[679]

UNESCO Rekomendācijā par mākslīgā intelekta ētiku kā būtiskākais instruments ir norādīts ētiskās ietekmes novērtējums, kas ir norādīta kā pirmā no vienpadsmit politikas darbības jomām.[680] Dalībvalstis tiek aicinātas ieviest šādu novērtējumu, kas ļautu izvērtēt mākslīgā intelekta sistēmu ieguvumus un riskus, kā arī šo risku novēršanas, samazināšanas un uzraudzības pasākumus. Rekomendācija uzsver, ka ir nepieciešams novērtēt mākslīgā intelekta plašāku ietekmi uz cilvēktiesībām un pamatbrīvībām, darba tiesībām, vidi un ekosistēmu, kā arī ētisko un sociālo ietekmi.

Eiropas Padome arī iesaka izmantot cilvēktiesību ietekmes novērtējumu un rekomendē dalībvalstīm izveidot tiesisko regulējumu, kas nosaka valsts iestāžu procedūru, lai veiktu šādu novērtējumu mākslīgā intelekta sistēmām, ko šīs iestādes iegūst, izstrādā vai izmanto. Cilvēktiesību ietekmes novērtējums būtu jāievieš un jāīsteno līdzīgi kā citi ietekmes novērtējumu veidi, ko veic valsts iestādes, piemēram, novērtējums par ietekmi uz datu aizsardzību.[681] Savukārt CAHAI priekšizpētes ziņojumā ir norādīts, ka Eiropas Padomes līmenī varētu tikt izstrādāta vienota metodika un norādījumi cilvēktiesību, demokrātijas un tiesiskuma

678 ANO Uzņēmējdarbības un cilvēktiesību pamatprincipos uzņēmumiem ir paredzēta cilvēktiesību atbilstības pārbaude – prasība ievērot cilvēktiesības, paredzot, ka uzņēmumiem jāidentificē, jānovērš, jāmazina un jāatskaitās par negatīvo ietekmi uz cilvēktiesībām, ko rada viņu darbība. Sk. OHCHR (2011), Guiding Principles on Business and Human Rights.

679 Mantelero, A. (2018). AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment. *Computer Law & Security Review*, 34(4), pp. 754–772. https://doi.org/10.1016/j.clsr.2018.05.017

680 UNESCO (2021), Recommendation on the Ethics of Artificial Intelligence.

681 Council of Europe Commissioner for Human Rights (2019), Unboxing Artificial Intelligence ..

ietekmes novērtējumam vai integrētajam ietekmes novērtējumam, ko varētu izmantot, lai apliecinātu atbilstību principiem, kas tiks noteikti nākotnes Eiropas Padomes tiesiskajā regulējumā.[682] Būtiski ir izvērtēt ietekmi ne tikai uz cilvēktiesībām, bet arī plašāku ietekmi uz tiesiskumu un demokrātiju.

Pēdējo gadu laikā ir izteikti daudzi priekšlikumi ieviest algoritmisko ietekmes novērtējumu (*algorithmic impact assessments* – angļu val.). Piemēram, *AI Now* institūts mudina veikt algoritmisko ietekmes novērtējumu ikvienai valsts iestādei, ne tikai policijai, pirms tā plāno izmantot automatizētu lēmumu pieņemšanas sistēmu.[683] Kanāda ir izstrādājusi algoritmisko ietekmes novērtējumu saskaņā ar Kanādas Direktīvu par automatizētu lēmumu pieņemšanu, ko var piemērot dažādos gadījumos.[684] Eiropas valstis izstrādā mākslīgā intelekta atbildības rīkus, galvenokārt pamatojoties uz esošajiem datu aizsardzības noteikumiem. 2020. gada februārī Apvienotās Karalistes datu aizsardzības iestāde ICO publicēja vadlīniju projektu par mākslīgā intelekta audita sistēmu.[685] Šiem novērtējumiem par paraugu noder esošie ietekmes novērtējumi, piemēram, ietekmes uz privātumu novērtējums, ētikas ietekmes novērtējums, vides ietekmes novērtējums un it īpaši VDAR paredzētais novērtējums par ietekmi uz datu aizsardzību.[686] Pamatā tie mēģina skaidrot, kā piemērot datu aizsardzības normas attiecībā uz mākslīgā intelekta sistēmām un sniegt ieteikumus organizatoriskiem un tehniskiem pasākumiem, lai mazinātu mākslīgā intelekta radītos riskus personām.

ES izstrādātie mākslīgā intelekta tiesiskā regulējuma priekšlikumi arī ir pamatā balstīti uz riska izvērtējumu, paredzot pienākumus attiecībā uz augsta riska tehnoloģijām. Eiropas Komisija 2020. gada Baltajā grāmatā norāda, ka, izstrādājot jauno regulējumu, tā vēlas piemērot uz risku balstīto pieeju. Ņemot vērā augsto risku, ko daži mākslīgā intelekta izmantošanas veidi rada iedzīvotājiem un mūsu sabiedrībai, būtu nepieciešams objektīvs, iepriekšējs atbilstības novērtējums, lai pārbaudītu un nodrošinātu, ka tiek ievērotas noteiktas obligātās prasības. Atbilstības iepriekšējā izvērtēšanā varētu iekļaut testēšanas, apskates vai sertifikācijas procedūras. Tā varētu ietvert izstrādes posmā izmantoto algoritmu un datu kopu pārbaudes.[687]

682 Council of Europe, CAHAI (2020), Feasibility Study.

683 Sk. Reisman et al. (2018). Algorithmic Impact Assessments Report: A Practical Framework for Public Agency Accountability. AI Now Institute. https://ainowinstitute.org/publication/algorithmic-impact-assessments-report-2

684 Government of Canada. Algorithmic Impact Assessment. https://canada-ca.github.io/aia-eia-js/

685 Kazim, E., Denny, D. M. T., Koshiyama, A. (2021). AI Auditing and Impact Assessment: According to the UK Information Commissioner's Office. *AI and Ethics*, 1, pp. 301–310. https://doi.org/10.1007/s43681-021-00039-2

686 Sk. Reisman et al. (2018), Algorithmic Impact Assessments Report.

687 Eiropas Komisija (2020), Baltā grāmata par mākslīgo intelektu.

Eiropas Parlamenta rezolūcijā ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru attiecībā uz riska novērtēšanu ir norādīts, ka jebkurā nākotnes regulējumā būtu jāievēro diferencēta, uz risku balstīta un uz nākotni vērsta pieeja mākslīgā intelekta, robotikas un saistīto tehnoloģiju regulēšanai, tostarp piemērojot tehnoloģiski neitrālus standartus visās nozarēs, kā arī vajadzības gadījumā nozarei specifiskus standartus. Lai garantētu riska novērtēšanas sistēmas vienveidīgu īstenošanu un to, ka dažādās dalībvalstīs tiek nodrošināti vienlīdzīgi konkurences apstākļi un netiek pieļauta iekšējā tirgus sadrumstalošanās, ir vajadzīgs izsmeļošs un kumulatīvs augsta riska nozaru un augsta riska lietojuma veidu vai nolūku saraksts. Lai noteiktu, vai šīm tehnoloģijām piemīt augsts risks un līdz ar to attiecināma prasība ievērot mākslīgā intelekta tiesiskajā regulējumā paredzētos juridiskos pienākumus, visos gadījumos būtu jāveic objektīvs, reglamentēts un ārējs sākotnējās ietekmes (*ex-ante*) novērtējums, kas balstīts uz konkrētiem un definētiem kritērijiem. Par augsta riska tehnoloģijām būtu jāuzskata tāds mākslīgais intelekts, robotika un saistītās tehnoloģijas, kuru izstrāde, ieviešana un izmantošana var radīt būtisku kaitējuma risku konkrētām personām vai sabiedrībai kopumā, pārkāpjot ES tiesību aktos noteiktās pamattiesības un drošības noteikumus. Vērtējot to, vai mākslīgā intelekta tehnoloģijas rada šādu risku, būtu jāņem vērā nozare, kurā tās tiek izstrādātas, ieviestas vai izmantotas, to konkrētais lietojums vai nolūks un paredzamais kaitējuma smagums. Uz risku balstītā pieeja būtu jāizstrādā tā, lai ierobežotu administratīvo slogu uzņēmumiem, cik vien iespējams izmantojot jau esošus instrumentus, piemēram, VDAR paredzēto sarakstu attiecībā uz prasību veikt novērtējumu par ietekmi uz datu aizsardzību.[688]

Eiropas Komisijas MI akta priekšlikums ietver specifiskus noteikumus attiecībā uz mākslīgā intelekta sistēmām, kuras rada augstu risku fizisku personu veselībai un drošībai vai pamattiesībām. Attiecībā uz šīm sistēmām ir paredzēts ieviest riska pārvaldības sistēmu, lai novērtētu zināmus un paredzamus mākslīgā intelekta riskus, kā arī noteiktu to samazināšanas un uzraudzības pasākumus.

Augsta riska mākslīgā intelekta sistēmas ir atļautas Eiropas tirgū, ja ir nodrošināta atbilstība noteiktām obligātām prasībām un veikta atbilstības priekšnovērtēšana. Mākslīgā intelekta sistēmas, kuras paredzēts izmantot kā drošības sastāvdaļas produktos, ir pakļautas trešo personu atbilstības priekšnovērtēšanai. Savukārt attiecībā uz citām savrupām mākslīgā intelekta sistēmām, kurām galvenokārt ir ietekme uz pamattiesībām un kuras ir skaidri uzskaitītas III pielikumā, tiks izveidota jauna atbilstības un izpildes sistēma. MI akta priekšlikums paredz,

688 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

ka sagādātājs[689] pirms laišanas tirgū vai nodošanas ekspluatācijā veic sistēmas atbilstības novērtēšanu (19., 43. pants). Kā izņēmums ir paredzēts biometriskas tālidentifikācijas sistēmas, uz kurām attiektos trešās personas veikta atbilstības novērtēšana. Pēc attiecīgās atbilstības novērtēšanas pabeigšanas sagādātājam būtu jāreģistrē minētās savrupās augsta riska mākslīgā intelekta sistēmas ES datubāzē.[690]

Eiropas Datu aizsardzības uzraudzītājs un Eiropas Datu aizsardzības kolēģija publicētajā kopīgajā viedoklī norāda, ka būtu nepieciešams pielāgot priekšlikuma atbilstības novērtēšanas procedūru, lai trešās personas vienmēr veiktu augsta riska mākslīgā intelekta sistēmu *ex-ante* atbilstības novērtējumus. Turklāt tās vērš uzmanību, ka jebkurā mākslīgā intelekta sistēmas riska novērtējumā būtu jāņem vērā tehniskie parametri, kā arī tās īpašie lietošanas gadījumi un konteksts, kurā sistēma darbojas. Iestādes ierosina priekšlikumā norādīt, ka pakalpojumu sniedzējs veic sākotnējo sistēmas riska novērtējumu, ņemot vērā lietošanas gadījumus, un ka sistēmas lietotājs, kas darbojas kā datu pārzinis saskaņā ar ES datu aizsardzības tiesību aktiem, ja nepieciešams, veic datu aizsardzības ietekmes novērtējumu, ņemot vērā ne tikai tehniskos parametrus un lietošanas gadījumu, bet arī konkrēto kontekstu, kurā mākslīgā intelekta sistēma darbosies. Turklāt minētās iestādes iesaka precizēt MI akta priekšlikumu, piemēram, papildinot III pielikuma 1. punkta a) apakšpunktu, ietverot tajā mākslīgā intelekta biometrisko sistēmu izmantošanas gadījumus.[691]

Mākslīgā intelekta ietekmes novērtējumi var būt nozīmīgi atbildības rīki, kas nodrošina, ka iestādes un uzņēmumi apzinās un novērtē savu tehnoloģiju riskus, izvērtējot to plašāku ietekmi uz cilvēktiesībām, demokrātiju, sociālo, ētisko un cita veida ietekmi. Tie var būt arī efektīvs instruments, lai sabiedrību un indivīdus informētu par šādu sistēmu izmantošanu un sniegtu viņiem informāciju, kas var palīdzēt noteikt, vai šīs sistēmas ir atbilstošas. Tajā pašā laikā ES mākslīgais intelekts nebūtu jāregulē, pamatojoties uz risku, bet gan pamatojoties uz cilvēktiesībām.

Mākslīgā intelekta regulējums nedrīkstētu paredzēt, ka iestādes un uzņēmumi paši novērtē savas darbības riskus cilvēktiesībām, sabiedrībai, demokrātijai. Tas

689 MI akta priekšlikums paredz, ka "sagādātājs" ir fiziska vai juridiska persona, publiskā sektora iestāde, aģentūra vai cita struktūra, kura par samaksu vai par brīvu izstrādā vai liek izstrādāt AI sistēmu laišanai tirgū vai nodošanai ekspluatācijā ar savu vārdu vai preču zīmi (3. panta 2. punkts).

690 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

691 EDPB, EDPS (2021), EDPB-EDPS Joint Opinion 5/2021 ..

būtu fundamentāli nepareizs priekšstats par to, kas ir cilvēktiesības, jo cilvēktiesības nevar sabalansēt ar uzņēmumu interesēm.[692]

Uz risku balstīta pieeja mākslīgā intelekta regulējumam nav pietiekama, lai aizsargātu cilvēktiesības. Gan valsts iestādes, gan uzņēmumi var nebūt ieinteresēti mazināt riskus, lai izstrādātu, ieviestu un izmantotu tehnoloģijas. Kaut arī jau šobrīd ES datu aizsardzības regulējums uzliek pienākumu novērtēt mākslīgā intelekta novērošanas tehnoloģiju ietekmi uz personas tiesībām un brīvībām, kā apliecina daudzi prakses gadījumi, šis mehānisms efektīvi nenovērš tādu tehnoloģiju ieviešanu, kas pārkāpj datu aizsardzības prasības un personu tiesības.[693] Lai gan ES datu aizsardzības regulējums tieši neparedz ietekmes uz ES vērtībām, sabiedrību, tiesiskumu un demokrātiju izvērtējumu, sistēmas, kas rada kaitējumu šīm vērtībām, bieži vien pārkāpj arī personu tiesības un brīvības. Šis regulējums nosaka pienākumu novērtēt un novērst riskus personu tiesībām un brīvībām, tomēr praksē tas bieži vien netiek ievērots. Tāpēc uz risku balstīta pieeja mākslīgā intelekta regulējumam nav pietiekama, lai aizsargātu cilvēktiesības. Cilvēktiesības nav apspriežamas, un tās ir jāievēro neatkarīgi no riska līmeņa.

Neatkarīgai uzraudzības iestādei vajadzētu būt pilnvarām uzdot un uzraudzīt ietekmes novērtējuma veikšanu gan *ex-ante*, gan regulāri, kad sistēmas tiek izmantotas. Tas ir svarīgi divos gadījumos: ja pastāv draudi cilvēktiesībām un ja mākslīgā intelekta vai automatizēta lēmumu pieņemšanas sistēmas var būt neprognozējamas.[694]

Turklāt gadījumos, kad mākslīgā intelekta tehnoloģijas rada būtiskus vai neprognozējamus riskus cilvēktiesībām, sabiedrībai, demokrātijai, tiesiskumam un citām pamatvērtībām un esošajā tiesiskajā regulējumā nav piemērotu pasākumu, kas šos riskus novērstu, minētās tehnoloģijas būtu jāaizliedz vai jānosaka to pagaidu aizliegums, nosakot to tiesiskā regulējumā, nevis jāgaida, kad tas tiks paredzēts katrā konkrētajā gadījumā, kad tiek veikts ietekmes novērtējums. Attiecībā uz tādu augsta riska tehnoloģiju izmantošanu tiesībaizsardzības nolūkos kā sejas atpazīšanas tehnoloģijas un prognozējošās tehnoloģijas būtu jānosaka vispārējs aizliegums, atļaujot tās izmantot tikai izņēmuma gadījumos un paredzot efektīvus uzraudzības mehānismus, tostarp *ex-ante* izvērtēšanu, ko veic neatkarīga uzraudzības iestāde.

Būtu jāizveido efektīva pārvaldības sistēma, kas ietvertu tādas neatkarīgas uzraudzības iestādes izveidi, kura pilnvarota veikt vai pārraudzīt mākslīgā

692 Hidvegi, F., Leufer, D., Massé, E. (17 February, 2021). The EU should regulate AI on the basis of rights, not risks. *Access Now*. https://www.accessnow.org/eu-regulation-ai-risk-based-approach/

693 Sk., piemēram, EDPB (21 February, 2021), Swedish DPA ..

694 Hidvegi, Leufer, Massé (17 February, 2021), The EU should regulate AI ..

intelekta sistēmu novērtēšanu un īstenot efektīvus kontroles mehānismus. Turklāt būtu jāparedz arī plašas sabiedrības līdzdalības iespējas.

7.6. Neatkarīga uzraudzība, sabiedrības līdzdalība un atbildība

Lai nodrošinātu kontroli pār mākslīgā intelekta sistēmu izmantošanu, novērstu to radīto apdraudējumu cilvēktiesībām, tiesiskumam un demokrātijai, ir nepieciešams izveidot efektīvu, pārredzamu, sabiedrību iekļaujošu uzraudzības mehānismu.[695] Valstīm ir jāizveido kontroles mehānismi un jānodrošina efektīvi tiesiskās aizsardzības līdzekļi, lai nodrošinātu, ka mākslīgā intelekta attīstība un izmantošana atbilst tiesiskām prasībām.[696]

Eiropas līmenī ir izteikti daudzi priekšlikumi izveidot neatkarīgu uzraudzības iestādi, kas pārraudzītu, vai mākslīgā intelekta sistēmas darbojas, ievērojot cilvēktiesības un citas tiesiskās prasības. Eiropas Padomes cilvēktiesību komisārs 2019. gada rekomendācijā rosina valstis pieņemt tiesisko regulējumu, kas noteiktu neatkarīgu un efektīvu uzraudzības iestādi, kura pārraudzītu cilvēktiesību ievērošanu attiecībā uz mākslīgā intelekta sistēmu izstrādi, ieviešanu un izmantošanu, ko veic valsts iestādes un privātās organizācijas. Uzraudzības iestādēm ir jābūt neatkarīgām no valsts iestādēm un privātām organizācijām, kas izstrādā, ievieš vai citādi izmanto mākslīgā intelekta sistēmas, tām ir jābūt atbilstošai starpdisciplinārai kompetencei un resursiem, lai veiktu uzraudzības funkciju.[697] Rekomendācijā norādīts, ka šīm iestādēm būtu proaktīvi jāizmeklē un jāuzrauga mākslīgā intelekta sistēmu atbilstība cilvēktiesībām, jāsaņem un jārisina aizskarto personu sūdzības, kā arī periodiski vispārīgi jāpārskata mākslīgā intelekta sistēmu iespējas un tehnoloģiskā attīstība. Tām jāpiešķir pilnvaras iejaukties apstākļos, kad tās konstatē iespējamus cilvēktiesību pārkāpumus. Uzraudzības iestādēm būtu arī regulāri jāatskaitās parlamentam vai citām iestādēm un jāpublicē ziņojumi par savu darbību. Valsts iestādēm un privātiem uzņēmumiem pēc pieprasījuma vajadzētu sniegt informāciju, kas nepieciešama efektīvai mākslīgā intelekta sistēmu uzraudzībai, kā arī regulāri jāziņo uzraudzības iestādēm. Tām būtu jāīsteno uzraudzības iestāžu sniegtie ieteikumi attiecībā uz mākslīgā intelekta sistēmu ietekmi uz cilvēktiesībām. Uzraudzības procesam jābūt pārredzamam un pakļautam atbilstošai sabiedrības kontrolei. Uzraudzības iestāžu lēmumiem ir jābūt neatkarīgi pārvērtējamiem vai pārsūdzamiem.[698]

695 Council of Europe, CAHAI (2020), Feasibility Study.

696 Ibid.

697 Council of Europe Commissioner for Human Rights (2019), Unboxing Artificial Intelligence ..

698 Ibid.

Līdzīgi arī CAHAI priekšizpētes ziņojumā tiek uzsvērts, ka Eiropas Padomes dalībvalstīm vajadzētu noteikt un pilnvarot neatkarīgas struktūras, kas veiktu uzraudzību. Tās pārstāvētu un atskaitītos skaidri identificētai grupai ieinteresēto personu, kuras ietekmē mākslīgā intelekta praktiskā izmantošana. Tās varētu būt ekspertu komitejas, akadēmiskās vides pārstāvji, nozaru uzraudzības iestādes vai privātā sektora auditori. Tāpat valstis varētu apsvērt iespēju izveidot neatkarīgas uzraudzības iestādes, kurām būtu atbilstošas starpdisciplinārās zināšanas, pilnvaras un resursi to funkciju veikšanai. Ziņojumā norādīts, ka ir svarīgi atzīt arī esošo nacionālo cilvēktiesību, līdztiesības un ombuda institūciju nozīmīgo lomu, lai nodrošinātu efektīvu uzraudzību. Valstis varētu paplašināt esošo institūciju pilnvaras vai arī izveidot jaunas iestādes, kas izskatītu visas sūdzības, kā papildu mehānismu tiesību aizsardzībai tiesā. Tomēr nevar gaidīt, ka jebkura šāda struktūra varētu aptvert pilnīgi visus produktus un pakalpojumus, kas balstīti uz mākslīgo intelektu, un tāpēc būtu svarīgi ņemt vērā darbības jomu. Ja tiek izveidotas jaunas iestādes, to pilnvarām nevajadzētu pārklāties vai nonākt konfliktā ar iepriekš pastāvošo iestāžu pārraudzības funkcijām, kas aptver mākslīgā intelekta sistēmu īpašu izmantošanas veidu pārraudzību.

Ziņojumā vērsta uzmanība uz pienākumu valstīm uzraudzīt mākslīgā intelekta sistēmu izmantošanu publiskā sektora iestādēs. Mākslīgā intelekta sistēmu publiskajam iepirkumam būtu jāpiemēro atbilstoši uzraudzības mehānismi, nosakot juridiski saistošas prasības, kas nodrošina mākslīgā intelekta atbildīgu izmantošanu publiskajā sektorā. Daudzi publiskie dalībnieki mākslīgā intelekta sistēmas iegādājas no privātiem dalībniekiem un paļaujas uz tiem, lai iegūtu datus, ieviestu mākslīgā intelekta sistēmas un piekļūtu infrastruktūrai, kas ir pamatā un nodrošina mākslīgā intelekta sistēmas darbību. Privātajiem dalībniekiem ir pienākums nodrošināt, ka to sistēmas tiek izstrādātas un izmantotas atbilstoši prasībām. Uzraudzības iestādēm vajadzētu būt pilnvarām uzlikt privātajiem dalībniekiem pienākumu ievērot tiesiskās prasības mākslīgā intelekta kontekstā, it īpaši, ja pastāv risks, ka to intereses atšķiras no indivīdu un sabiedrības interesēm. Turklāt jānodrošina piekļuve tiesai, ja šie dalībnieki nepilda tiem uzliktos pienākumus.[699]

Arī ES līmenī ir vērsta uzmanība uz nepieciešamību izveidot neatkarīgu uzraudzības iestādi. Eiropas Parlamenta Regulas par mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrādes, ieviešanas un izmantošanas ētikas principiem priekšlikumā paredzēts, ka dalībvalstīm būtu jāizraugās neatkarīga administratīva iestāde, kas darbotos kā uzraudzības iestāde. Valsts uzraudzības iestādes palīdzētu nodrošināt regulas konsekventu piemērošanu visā ES, sadarbojoties gan savā starpā, gan ar ES iestādēm. Katra valsts uzraudzības iestāde darbotos kā

699 Council of Europe, CAHAI (2020), Feasibility Study.

pirmais kontaktpunkts gadījumos, kad rodas aizdomas par regulā noteikto ētikas principu un juridisko pienākumu pārkāpšanu, tostarp par diskriminējošu attieksmi vai citu tiesību pārkāpšanu, mākslīgā intelekta, robotikas un saistīto tehnoloģiju izstrādes, ieviešanas vai izmantošanas rezultātā. Šādos gadījumos attiecīgā valsts uzraudzības iestāde veic atbilstības novērtējumu, lai atbalstītu pilsoņu tiesības apstrīdēt un panākt savu tiesību aizsardzību. It īpaši uzraudzības iestādei vajadzētu būt atbildīgai par augsta riska mākslīgā intelekta tehnoloģiju apzināšanu un par šo tehnoloģiju atbilstības novērtēšanu un uzraudzību. Lai novērtētu un uzraudzītu augsta riska tehnoloģiju atbilstību, valsts uzraudzības iestādēm būtu jāsadarbojas arī ar citām iestādēm, kuras ir atbildīgas par reglamentējošu tiesību aktu nodrošināšanu saistītās nozarēs. Valsts uzraudzības iestādei būtu jānodrošina forums, kurā notiek regulāra viedokļu apmaiņa ar ieinteresētajām personām no akadēmiskajām aprindām, pētniecības vides, nozares un pilsoniskās sabiedrības un minēto personu starpā.[700]

ES MI akta priekšlikums paredz izveidot Eiropas Mākslīgā intelekta padomi, kurā piedalītos dalībvalstu un Eiropas Komisijas pārstāvji, kas veicinātu regulas netraucētu, efektīvu un saskaņotu īstenošanu, sekmējot valstu uzraudzības iestāžu un Eiropas Komisijas produktīvu sadarbību. Minētais priekšlikums paredz, ka valstu līmenī dalībvalstīm būs jānorīko viena vai vairākas valsts kompetentās iestādes, savukārt no to vidus – valsts uzraudzības iestāde regulas piemērošanas un īstenošanas uzraudzībai. Eiropas Datu aizsardzības uzraudzītājs savukārt darbosies kā kompetentā iestāde ES iestāžu, aģentūru un struktūru uzraudzībai.[701]

FRA norāda, ka ES ir labi attīstīts neatkarīgu institūciju kopums, kuru pilnvaras aizsargā un veicina pamattiesības, tās ir datu aizsardzības iestādes, līdztiesības organizācijas, valstu cilvēktiesību institūcijas un ombuda iestādes. FRA veiktais pētījums parāda, ka tie, kas izmanto vai plāno izmantot mākslīgo intelektu, bieži sazinās ar dažādām iestādēm par to izmantošanu, piemēram, datu aizsardzības iestādēm un patērētāju tiesību aizsardzības iestādēm.[702] Ne vienmēr var būt skaidrs, kura iestāde ir atbildīga par mākslīgā intelekta sistēmu uzraudzību. Visbiežāk mākslīgā intelekta izmantotāji sazinājušies ar datu aizsardzības iestādēm, lai iegūtu padomus, ieteikumus vai apstiprinājumu gadījumos, kad notiek personas datu apstrāde. Tomēr datu aizsardzības iestādēm šim uzdevumam nav pietiekamu resursu un tām trūkst īpašu zināšanu mākslīgā intelekta jautājumos. Ir jāpastiprina esošo uzraudzības iestāžu personāla zināšanas, lai tās varētu efektīvi uzraudzīt ar mākslīgo intelektu saistītos jautājumus, kas var būt izaicinājums.

700 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

701 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

702 FRA. (2020). Getting the future right. Artificial intelligence and fundamental rights. https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

Uzraudzības iestādēm ir jāpiešķir pietiekami resursi, pilnvaras un jānodrošina kompetence, lai novērstu un novērtētu pamattiesību pārkāpumus un efektīvi atbalstītu personas, kuru pamattiesības skar mākslīgais intelekts.

FRA uzsver arī sabiedrības līdzdalības nozīmi. Mākslīgā intelekta ietekmes uz cilvēktiesībām novērtējums varētu būt par pamatu konsultācijām ar dažādām ieinteresētajām personām un ekspertiem pirms konkrētās mākslīgā intelekta sistēmas izmantošanas. Apspriešanās ar attiecīgajām ieinteresētajām personām var nodrošināt, ka nepaliek nepamanīts iespējamais kaitējums un ka novērtējums tiek veikts no dažādām perspektīvām. Ieinteresētās puses varētu būt pilsoniskā sabiedrība, dažādas valsts un privātās organizācijas, kā arī cilvēktiesību un datu aizsardzības eksperti. Pilsoniskās sabiedrības organizācijām, kas specializējas tehnoloģiju, digitālo tiesību un algoritmu jomā, ir nozīmīga loma, lai veicinātu atbildīgu mākslīgā intelekta sistēmu izmantošanu. Efektīvai mākslīgā intelekta sistēmu uzraudzībai ir nepieciešama cieša sadarbība starp visām ieinteresētajām pusēm – valsts iestādēm, kurām jānodrošina pārraudzība, privātiem dalībniekiem, kuri var sniegt savas zināšanas un izstrādāt mākslīgā intelekta sistēmas, kas sniedz labumu sabiedrībai, kā arī pilsoniskās sabiedrības organizācijām, kas var pārstāvēt dažādu sabiedrības grupu intereses.[703]

A. Mantelero norāda, ka, ņemot vērā kolektīvo dimensiju, kāda ir datu izmantošanai mākslīgā intelekta sistēmās, cilvēku kontrole un uzraudzība nevar aprobežoties tikai ar uzraudzības iestādēm, datu apstrādātājiem vai datu subjektiem. Līdzdalības un demokrātiskas uzraudzības procedūrai būtu jādod balss sabiedrībai kopumā, tostarp dažādām cilvēku kategorijām, minoritātēm un nepietiekami pārstāvētām grupām. Arī ietekmes novērtējuma veikšanā būtu jāparedz sabiedrības līdzdalība. Būtu jāizstrādā riska novērtēšanas līdzdalības formas, aktīvi iesaistot iespējami skartās personas un grupas. Indivīdi, grupas un citas ieinteresētās personas būtu jāinformē un aktīvi jāiesaista debatēs par lomu, kādu mākslīgais intelekts ieņem sociālās dinamikas veidošanā un lēmumu pieņemšanas procesos, kas attiecīgās personas ietekmē. Atkāpes var paredzēt sabiedrības interesēs, ja tās ir proporcionālas demokrātiskā sabiedrībā un ja tiek nodrošinātas atbilstošas garantijas. Policijas, izlūkošanas un drošības jomā, kur sabiedrības uzraudzība ir ierobežota, valdībai ir regulāri jāziņo par mākslīgā intelekta izmantošanu.[704]

Aprakstītā neatkarīgā uzraudzība, kas paredz arī sabiedrības līdzdalību, ir tā sauktais stratēģiskais uzraudzības līmenis. Tam līdzās pastāv taktiskais uzraudzības līmenis, kas paredz noteikumus, kuri ir pieņemti attiecībā uz sistēmas izmantošanu noteiktos nolūkos un kuri paredz prasības, kādas ir jāievēro katrā

703 Council of Europe, CAHAI (2020), Feasibility Study.

704 Mantelero (2020), Regulating AI within the Human Rights Framework, p. 489.

konkrētajā gadījumā.[705] Novērošanas tehnoloģijām būtiska prasība ir iepriekšēja tiesneša akcepta jeb ordera saņemšana, kas ļauj veikt mērķtiecīgu novērošanu nacionālās drošības nolūkā, izmantojot, piemēram, sejas atpazīšanas tehnoloģijas. Šāda mehānisma izveidošana kā būtiska garantija pret negodprātīgu praksi un varas ļaunprātīgu izmantošanu izriet arī no ECT un EST prakses masveida novērošanas lietās, kas analizētas iepriekš grāmatas piektajā nodaļā.

Attiecībā uz taktisko uzraudzību sabiedrības līdzdalība ir stingri ierobežota. Bieži vien sabiedrība par to uzzina, kad persona iesniedz sūdzību uzraudzības iestādē vai tiesā vai, piemēram, ja tiek publicēta slēpta informācija, kā tas notika Snoudena atklājumu gadījumā. Vienlaikus arvien vairāk tiek pieprasīts, lai valsts iestādes informē sabiedrību par jauno tehnoloģiju izmantošanas praksi, īpaši tad, ja tās aizskar cilvēktiesības.

Neatkarīgas uzraudzības iestādes kontrole, kā arī visas sabiedrības pārraudzība ir sevišķi būtiska attiecībā uz augsta riska mākslīgā intelekta tehnoloģijām, kādas ir sejas atpazīšanas un citas masveida novērošanas tehnoloģijas. Ir nepieciešamas plašas debates, iesaistot ne tikai valsts iestādes, bet arī pilsonisko sabiedrību un zinātniekus, kurās būtu jārisina jautājumi gan par atbildības prasībām, kas piemērojamas mākslīgajam intelektam, gan plašāk par to, kādas ir biometriskās novērošanas un citu mākslīgā intelekta tehnoloģiju izmantošanas sarkanās līnijas. Uzraudzības un sabiedrības līdzdalības mehānismi kopā ļauj apturēt tādu tehnoloģiju ieviešanu un izstrādi, kas pārkāpj cilvēktiesības un demokrātijas principus, kā arī citas tiesiskās prasības. Par mākslīgā intelekta masveida novērošanas sistēmu atbilstību būtu jālemj nevis tikai policijai vai citām tiesībaizsardzības iestādēm, bet gan neatkarīgām uzraudzības iestādēm, iesaistot visu sabiedrību, un tām arī iepriekš jānovērtē, vai pastāv līdzsvars starp privātuma un drošības interesēm. Pilsoņu līdzdalībai ir būtiska loma, lai nodrošinātu lēmumu pārredzamību un atbildību, kā arī pasargātu personas no nelikumīgas novērošanas un atklātu prettiesisku praksi. Lai varētu efektīvi īstenot uzraudzību un sociālo līdzdalību, mākslīgā intelekta sistēmām ir jābūt arī pārredzamām.

7.7. Pārredzamība un informēšana

Mākslīgā intelekta sistēmu izmantošana bieži tiek slēpta vai nav zināma, tāpēc ir grūti vai neiespējami izvērtēt to ietekmi un uzraudzīt, vai tās tiek izmantotas tiesiski. Bez pārredzamības ir grūti noteikt, vai ir pārkāptas cilvēktiesības. Ja persona un sabiedrība kopumā nezina, ka to cilvēktiesības tiek aizskartas, tā nevar arī tās aizsargāt.

705 Schneier (2016), *Data and Goliath* .., pp. 189–190.

Sejas atpazīšanas un citas mākslīgā intelekta novērošanas tehnoloģijas bieži vien tiek izmantotas slepeni, arī Eiropā. Sabiedrībai ir maz zināms, kādas tehnoloģijas tiek izmantotas un kādā veidā, vai ir pierādījumi, ka tās tiešām ir vajadzīgas, un kas to apliecina. Šāda informācija ir jāatklāj gan uzraudzības iestādēm, gan sabiedrībai. Pārredzamības princips nodrošina cilvēka kontroli pār tehnoloģiju izmantošanu, lai mākslīgā intelekta sistēmas varētu pārbaudīt, saskaņot ar personu vēlmēm un ļautu personām, kuras šīs sistēmas ietekmē nelabvēlīgi, apstrīdēt to iznākumu.

Lēmumi, kas attiecas uz mākslīgā intelekta un citu jauno tehnoloģiju izmantošanas veidu, kuri var negatīvi ietekmēt cilvēktiesības un demokrātiju, kādas nepārprotami ir sejas atpazīšanas un cita veida novērošanas tehnoloģijas, nevar tikt pieņemti slepeni, bet gan par to ir jābūt atklātām diskusijām ar sabiedrību, sniedzot visu nepieciešamo informāciju, kas ļautu izvērtēt šo tehnoloģiju radīto ietekmi un to, vai šīm sistēmām var uzticēties. Ir vajadzīga plaša un stingra sabiedrības kontrole un visaugstākais iespējamais pārredzamības līmenis, kas sniegtu vispārēju pārskatu par mākslīgā intelekta tehnoloģiju izmantošanu tiesībaizsardzības jomā, kā arī ļautu veikt mākslīgā intelekta novērošanas tehnoloģiju risku novērtējumu.[706] Gatavojoties īstenot atbilstības, pārskatatbildības un kompensācijas pasākumus, vispirms ir jānodrošina mākslīgā intelekta sistēmu izmantošanas pārredzamība, jo tas var ietekmēt cilvēktiesības, demokrātiju un tiesiskumu.[707]

Pārredzamības prasības ir jānodrošina visas mākslīgā intelekta sistēmas uzraudzības laikā, un tas var ietvert gan pienākumu publiski izpaust informāciju par attiecīgo sistēmu, tās procesiem, tiešo un netiešo ietekmi uz cilvēktiesībām, gan par pasākumiem, kas veikti, lai identificētu un mazinātu sistēmas nelabvēlīgo ietekmi uz cilvēktiesībām. Pārredzamību var īstenot, arī veicot neatkarīgu, visaptverošu un efektīvu auditu. Visos gadījumos publiskotajai informācijai vajadzētu ļaut jēgpilni novērtēt mākslīgā intelekta sistēmu. Nevienai mākslīgā intelekta sistēmai nevajadzētu būt tik sarežģītai, lai tā nepieļautu cilvēku pārbaudi. Nedrīkstētu izmantot sistēmas, kas nevar nodrošināt atbilstošas pārredzamības un pārskatatbildības prasības.[708]

Tiesiskajā regulējumā būtu jāparedz skaidras pārredzamības prasības. Tas varētu ietvert tiesisku pienākumu publicēt mākslīgā intelekta sistēmu ietekmes novērtējumu, kā arī publisko konsultāciju atzinumu, kas atspoguļo ekspertu un sabiedrības pārstāvju paustos viedokļus, īpaši attiecībā uz augsta riska tehnoloģijām. Varētu tikt paredzēta prasība darīt pieejamu informāciju, kas ļautu

706 Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ..

707 Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence.

708 Council of Europe Commissioner for Human Rights (2019), Unboxing Artificial Intelligence ..

uzraudzības iestādēm izvērtēt mākslīgā intelekta sistēmu atbilstību cilvēktiesībām, tiesiskumam un demokrātiskām vērtībām. Uzraudzības iestādei būtu arī jāizglīto un jāveicina sabiedrības izpratne par mākslīgā intelekta atbildības prasībām.

Viens no priekšlikumiem, kas būtiski veicinātu pārredzamību, ir mākslīgā intelekta sistēmu reģistra izveide. Dažādu policijas un citu tiesībaizsardzības iestāžu prakse var būt ļoti atšķirīga. Sejas atpazīšana tiek plaši izmantota dažādos kontekstos ar nelielu pārredzamību vai bez tās. Tāpēc būtu nepieciešams visu mākslīgā intelekta sistēmu vai automatizēto lēmumu pieņemšanas procesu reģistrs.[709] Valstīm vajadzētu izveidot sarakstu, kas ietvertu vismaz to mākslīgā intelekta tehnoloģiju izmantošanu, kas ir uzskatāmas par augsta riska tehnoloģijām saskaņā ar ES regulējumu. Reģistrā varētu tikt norādīta riska klase un nepieciešamais pārredzamības un atbildības apjoms konkrētai lietojumprogrammai.[710]

Reģistru varētu izveidot un uzturēt gan nacionālā līmenī, gan arī būtu atbalstāma ideja izveidot ES reģistru, kurā tiktu vienkopus atspoguļota informācija par visām ES dalībvalstīm. Lai uzlabotu publisko pārredzamību un pārraudzību un stiprinātu kompetento iestāžu veikto vēlāko uzraudzību, MI akta priekšlikums paredz ES līmenī izveidot augsta riska mākslīgā intelekta sistēmu datubāzi, kuru pārvaldīs Eiropas Komisija.[711]

Pārredzamība ir jānodrošina ne tikai mākslīgā intelekta sistēmu vispārējā uzraudzībā, bet arī attiecībā uz katru konkrēto mākslīgā intelekta izmantošanas gadījumu. Kā tika atklāts grāmatas iepriekšējā sestajā nodaļā, pārredzamības princips paredz, ka ikvienai personai ir tiesības būt pienācīgi informētai, kad viņa tieši mijiedarbojas ar mākslīgā intelekta sistēmu, saņemot viegli saprotamu un pieejamu informāciju par tās mērķi un sekām, tostarp par automatizētu lēmumu pieņemšanu. Mākslīgā intelekta sistēmas izmantošanai jābūt identificējamai jebkurā lēmumu pieņemšanas procesā, kas būtiski ietekmē personas cilvēktiesības. Katrai personai ir tiesības iesniegt pieprasījumu un uzzināt jebkura uz mākslīgo intelektu balstīta lēmuma pamatojumu, ja tāds ir pieņemts un attiecas uz šo personu.[712] Personām ir jāspēj saprast, kā tiek pieņemti lēmumi un kā šie lēmumi tiek pārbaudīti. Personām, attiecībā uz kurām valsts iestāde ir pieņēmusi lēmumu, tikai vai būtiski izmantojot mākslīgā intelekta sistēmas, vajadzētu par to paziņot un nekavējoties sniegt iepriekš minēto informāciju.[713]

709 Kayser-Bril (18 June, 2020), At least 11 police forces use face recognition ..

710 Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence.

711 Eiropas Komisija (2021), Priekšlikums. .. Mākslīgā intelekta akts.

712 Mantelero (2020), Regulating AI within the Human Rights Framework, p. 490.

713 Council of Europe Commissioner for Human Rights (2019), Unboxing Artificial Intelligence ..

Eiropas Padome vērš uzmanību, ka būtu aktīvi jāinformē personas un jāsekmē plaša sabiedrības izpratne par sejas atpazīšanas tehnoloģijām un to ietekmi uz pamattiesībām. Piemēram, sejas atpazīšanas tehnoloģiju integrēšana esošajās novērošanas sistēmās ne vienmēr paredz informēt tās personas vai sadarbības grupu pārstāvjus, kuru biometriskie dati tiek apstrādāti, piemēram, ja tiek apsvērta iespēja piekļūt personu digitālajiem attēliem internetā. Personām būtu vienkāršā veidā jāizskaidro tādi jēdzieni kā sensitīvie dati, biometriskie dati, kā darbojas sejas atpazīšana, kā arī jābrīdina par iespējamiem riskiem, kas var rasties neatļautas izmantošanas gadījumā. Likumdevējam un lēmumu pieņēmējiem būtu jāveicina sabiedrības iesaistīšanās sejas atpazīšanas tehnoloģiju izstrādes un izmantošanas uzraudzīšanā, kā arī piemērotu aizsardzības garantiju noteikšanā.[714]

Pārredzamība ir nepieciešama, lai radītu uzticēšanos mākslīgā intelekta sistēmām. Sabiedrības informēšana, kā arī plašas sabiedrības diskusijas var radīt šo uzticēšanos, kas ir pamats, lai sistēmas varētu ieviest, izmantot un lai sabiedrība tās pieņemtu, kā arī lai tās kalpotu sabiedrībai un tiktu novērsti to radītie riski.[715] Informētība un izglītotība ir būtisks nosacījums uzticama un uz cilvēku vērsta mākslīgā intelekta attīstībai. Sabiedrības izglītošana un izpratnes veidošana ir priekšnosacījums, lai personas apzinātos arī savu vērtību un tiesības un varētu tās aizsargāt.

7.8. Novērošanas tehnoloģiju uzraudzība pēc Covid-19 krīzes

Ir jārēķinās, ka pēc Covid-19 krīzes sabiedrība būs fundamentāli un neatgriezeniski pārveidota. Lai cīnītos ar pandēmiju, valstis visā pasaulē strauji sāka eksperimentēt ar digitālajām novērošanas tehnoloģijām. Grāmatas pirmajā nodaļā tika raksturotas dažāda veida tehnoloģijas, sākot no veselības lietotnēm, valkājamām aprocēm, kontaktu izsekošanas un citām mobilām lietotnēm, beidzot ar sejas atpazīšanas tehnoloģijām, ko valstis ieviesa ar mērķi nodrošināt sabiedrības veselību un drošību. Tāpat grāmatas iepriekšējās nodaļās[716] tika atklāts, ka šīs tehnoloģijas būtiski satricināja cilvēktiesības un lika pārvērtēt datu aizsardzības prasību piemērošanu. Šīs tehnoloģijas radīja daudz jaunu jautājumu par to, kā līdzsvarot privātumu ar sabiedrības drošības un veselības aizsardzības interesēm un pārredzamību, indivīdu intereses ar kolektīvajām interesēm, steidzamību ar

714 Council of Europe (2021), .. Convention 108.

715 Sk. OECD (2019), Recommendation of the Council on Artificial Intelligence.

716 Sk. grāmatas 1.2.5., 2.6., 3.6., 6.6. nodaļas.

pārdomātu rīcību. Tas, kā tiks atbildēts uz šiem jautājumiem, ilgtermiņā ietekmēs pilsoniskās brīvības, pārvaldību un tehnoloģiju lomu sabiedrībā.[717]

Valstīm būtu jāveido politika, kas nodrošinātu stingru uzraudzību pār šo tehnoloģiju ieviešanu un izmantošanu gan pandēmijas laikā, gan pēc tās. Krīze padarīja valdību lēmumu pieņemšanas procesu, tai skaitā jaunu tehnoloģiju un citu cilvēktiesību ierobežojošu pasākumu ieviešanu, daudz nedemokrātiskāku, slepenāku un nepārredzamāku. Šo tendenci var būt grūti apturēt. Grāmatas otrajā nodaļā tika pamatots, ka krīzes situācijā valstis nav atbrīvotas no cilvēktiesību ievērošanas. Līdzīgi krīze neatbrīvo valdības no prasības nodrošināt atbildīgu un demokrātisku jauno tehnoloģiju un citu pasākumu ieviešanu un uzraudzīt to turpmāku izmantošanu, nepieļaujot sarkano līniju pārkāpšanu. Iepriekš nodaļā aprakstītās garantijas – ietekmes izvērtēšanu, pārredzamību, informēšanu, neatkarīgu uzraudzību, sabiedrības līdzdalību – ir svarīgi ievērot, ieviešot jaunas tehnoloģijas arī krīzes situācijā. Tomēr daudzas no tehnoloģijām, to skaitā kontaktu izsekošanas lietotnes, tika ieviestas, nepastāvot skaidriem pierādījumiem par to efektivitāti vai pat standartiem, pēc kuriem izvērtēt efektivitāti. Skaidrs regulējums, kas paredzētu pienākumu ievērot minētās prasības, samazinātu iespēju, ka tās tiek ieviestas nepamatoti, neveicot to ietekmes izvērtējumu, kā arī novērstu to turpmāku izmantošanu pēc krīzes iepriekš neparedzētos nolūkos. Skaidrs regulējums, atbildības prasības un uzraudzības mehānismi ir būtiski ne tikai lai aizsargātu cilvēktiesības un demokrātiju, bet arī lai masveida novērošanas pasākumi nekļūtu par jauno normu.

Covid-19 krīze radīja ne tikai daudzus izaicinājumus, bet arī unikālu iespēju pārvērtēt tehnoloģiju ieviešanas un demokrātiskas pārvaldības politiku, procesus un sadarbības iespējas. Tā radīja daudzus pozitīvus piemērus efektīvai un ātrai valsts un privāto uzņēmumu sadarbībai ar mērķi sniegt kopīgu labumu sabiedrībai. Krīze liek domāt ārpus tradicionālās pieejas, veicinot starpdisciplināru, starpsektoru un starptautisko sadarbību. Tā liek pārdomāt attiecības starp digitālās suverenitātes aizsardzību un tehnoloģiju uzņēmumu datu vākšanu un analīzi.[718] Tā liek pievērst pastiprinātu uzmanību jautājumiem, kā nodrošināt gan valsts iestāžu, gan privāto uzņēmumu atbildību, piemēram, gadījumos, kad valsts sadarbojas ar tehnoloģiju uzņēmumiem, kas piedalās datu vākšanā un jauno tehnoloģiju nodrošināšanā, ņemot vērā, ka praksē lielā mērā tie nav pakļauti atbildības prasībām. Tā var likt izvērtēt jauno tehnoloģiju patiesās iespējas un tās nepārvērtēt. Krīze var likt pārdomāt arī jauno tehnoloģiju ietekmi uz cilvēktiesībām, to

717 Social Science Research Council. (2021). Surveillance and the 'New Normal' of Covid-19: Public Health, Data, and Justice. https://covid19research.ssrc.org/public-health-surveillance-and-human-rights-network/report/

718 Ibid.

ierobežošanu tādu sabiedrības interešu vārdā kā drošība un veselība. Principi un procesi, kas rodas šādas izvērtēšanas rezultātā, var atšķirties atkarībā no sabiedrībā pastāvošajām vērtībām. Ārkārtas apstākļi var arī veicināt mākslīgā intelekta uzticamību un atbildību, ieviešot mehānismus, kas iedzīvina praksē cilvēktiesības, tiesiskumu un demokrātijas principus.

Kopsavilkums

Mākslīgais intelekts rada jaunus apdraudējumus cilvēktiesībām, tiesiskumam un demokrātijai. Straujā mākslīgā intelekta attīstība ievērojami veicina novērošanas sabiedrības izveidi. Mākslīgā intelekta tehnoloģijas būtiski palielina varas nevienlīdzību gan no valsts, gan lielo tehnoloģiju uzņēmumu puses, ko vairs nedrīkst ignorēt. Arī pirms mākslīgā intelekta, kā to spilgti parāda Edvarda Snoudena atklājumi, valstis ir patvaļīgi izmantojušas tehnoloģijas un personas datus, lai slepeni veiktu masveida novērošanu, atsaucoties uz valsts un sabiedrības drošības aizsardzības interesēm, radot būtisku aizskārumu personu tiesībām uz privātumu, datu aizsardzību un citām cilvēka pamattiesībām. Kā liecina prakse, šādus pasākumus atcelt ir ļoti grūti, dažkārt pat neiespējami, un bieži vien tam ir nepieciešamas ilgstošas tiesvedības.

Mākslīgā intelekta novērošanas tehnoloģijas var radīt daudz ievērojamāku apdraudējumu. Gan Eiropā, gan citviet pasaulē valsts iestādes arvien plašāk ievieš sejas atpazīšanas, emociju uztveršanas un citas biometriskās sistēmas, kā arī prognozēšanas metodes tiesībaizsardzības nolūkos. Šīs sistēmas tiek izmantotas, lai veiktu masveida novērošanu, atsaucoties uz tādu būtisku sabiedrības interešu aizsardzību kā nacionālā drošība un sabiedriskā drošība. Arvien biežāk minētās sistēmas tiek izmantotas, lai izdarītu secinājumus un prognozes par cilvēku uzvedību, domām un citām personiskām īpašībām, kā arī, balstoties uz šīm prognozēm, tiek pieņemti lēmumi, kas var radīt personai nelabvēlīgas sekas. It īpaši autoritārās valstīs tās arvien vairāk izmanto sociālajai vērtēšanai, slēptai manipulācijai un cilvēku uzvedības kontrolei. Valstis vairs nevar ignorēt šādu mākslīgā intelekta tehnoloģiju izmantošanu, un būtu jāpieņem jauns juridiski saistošs regulējums, kas noteiktu stingrus ierobežojumus un aizliegtu tādas darbības, kuras ir pretrunā cilvēktiesībām, tiesiskumam un demokrātiskām pamatvērtībām.

Starptautiskās un Eiropas organizācijas plaši diskutē un meklē piemērotākos veidus, kā regulēt mākslīgo intelektu, un strauji izstrādā tiesisko regulējumu. Ir svarīgi nepalaist garām šo izšķirošo brīdi, kad starptautiskā un Eiropas līmenī ir iespējams noteikt skaidras sarkanās līnijas tāda mākslīgā intelekta izmantošanai, kas pārkāpj cilvēktiesības.

Regulējums, kas tiks pieņemts tuvākajos gados, noteiks turpmāko mākslīgā intelekta attīstību. Mēs atrodamies krustcelēs, kur ir iespējams izvēlēties, pa kuru no diviem ceļiem gribam iet. Vai vēlamies iet pa ceļu, pa kuru mūsu sejas attēlus fiksē sejas atpazīšanas tehnoloģijas, kas tos salīdzina ar plašām datubāzēm un analizē, vai mēs neesam izdarījuši vai neplānojam izdarīt noziedzīgu nodarījumu

vai likumpārkāpumu. Šo tehnoloģiju algoritmi daudz neprecīzāk darbojas attiecībā pret konkrētu grupu pārstāvjiem, veicinot diskrimināciju. Mūsu rīcības brīvība var tikt ierobežota, piemēram, izvēlē piedalīties pret valdību vērstās protesta akcijās, jo par to varam tikt sodīti, tāpēc ka tehnoloģijas ļaus identificēt protesta dalībniekus. Vai gribam, ka mūsu emocijas, jūtas, domas un uzvedību analizē mākslīgā intelekta algoritmi un ka, pamatojoties uz to rezultātiem, tiek pieņemti lēmumi, kas var radīt būtiskas sekas, piemēram, arestēšanu, pabalsta atteikšanu, atlaišanu no darba, neuzņemšanu augstskolā?

Vai arī mēs izvēlēsimies iet pa otru ceļu, kur mākslīgā intelekta sistēmas ir stingri regulētas, nosakot skaidrus ierobežojumus un sarkanās līnijas tādu tehnoloģiju izmantošanai, kas pārkāpj vai var būtiski aizskart cilvēktiesības, tiesiskumu un demokrātiju, kā arī skaidras aizsardzības garantijas, lai kontrolētu šo tehnoloģiju izmantošanu. Ejot pa šo ceļu, jau pirms tiek izstrādātas un ieviestas mākslīgā intelekta un citas jaunās tehnoloģijas, kas var radīt riskus un apdraudējumu cilvēktiesībām un pamatbrīvībām, ir jāpierāda to nepieciešamība, efektivitāte un samērīgums un neatkarīgai uzraudzības iestādei ir jāveic šo tehnoloģiju ietekmes novērtējums, iesaistot un uzklausot arī sabiedrības, nevalstisko organizāciju, dažādu grupu, kuras šīs tehnoloģijas var aizskart, pārstāvju un dažādu jomu ekspertu viedokļus. Novērtējumi visiem ir publiski pieejami. Tiek rūpīgi kontrolēts un uzraudzīts, vai esošās mākslīgā intelekta sistēmas tiek izmantotas atbildīgi un likumīgi, stingri ievērojot tiesiskā regulējuma prasības, tostarp datu aizsardzības noteikumus. Mākslīgā intelekta novērošanas tehnoloģiju izstrāde nenotiek slepeni, un tās netiek negaidīti ieviestas vai slepeni izmantotas, bet gan tiek publiskoti brīdinājumi, kas ikvienam sniedz saprotamu un skaidru informāciju par to izmantošanu. Mākslīgā intelekta sistēmu reģistrā var atrast informāciju par tādu mākslīgā intelekta sistēmu izmantošanu, kas var radīt augstu risku. Ir izveidoti mehānismi, lai personām, kuru tiesības un brīvības šo tehnoloģiju izmantošana apdraud, ir iespējams kolektīvi tās aizstāvēt un saņemt atbilstīgu atlīdzinājumu.

Šī izvēle netiek izdarīta vienā dienā. Mēs pastāvīgi veicam daudz dažādu izvēļu, turklāt krīzes situācijās var būt grūtāk izdarīt pareizās. Covid-19 pandēmija ievērojami pastiprināja masveida novērošanas tendenci. Visā pasaulē valstis strauji eksperimentēja ar dažādām digitālām tehnoloģijām, sākot no kontaktu izsekošanas lietotnēm, digitālajiem sertifikātiem, līdz pat valkājamām aprocēm, droniem un sejas atpazīšanas tehnoloģijām, lai kontrolētu iedzīvotāju pārvietošanos ar mērķi ierobežot vīrusa izplatību. Jāatceras, ka nekas nav tik paliekošs kā pagaidu pasākumi. Ir rūpīgi jāuzrauga jaunu tehnoloģiju un pasākumu, kas ierobežo cilvēktiesības, ieviešana un izmantošana, paredzot efektīvas aizsardzības garantijas, lai nepieļautu nesamērīgu cilvēktiesību ierobežošanu, kā arī lai masveida novērošana nekļūtu par jauno normu.

Tajā pašā laikā Covid-19 krīze radīja arī unikālu iespēju izvērtēt jauno tehnoloģiju nozīmi un kritiski skatīties uz to sniegtajām iespējām un efektivitāti. Tā lika pārvērtēt demokrātiskas pārvaldības politiku un procesus, cita starpā atklājot nepilnības attiecībā arī uz veidu, kādā valstī tiek ieviestas, izmantotas, izvērtētas un uzraudzītas jaunās tehnoloģijas. Tā atklāja arī to, cik ietekmīgs līdzeklis jaunās tehnoloģijas var kļūt valsts rokās, lai kontrolētu sabiedrību un ierobežotu cilvēktiesības, un kādus riskus un apdraudējumus tās var radīt.

Lai veicinātu uzticama, atbildīga un uz cilvēku vērsta mākslīgā intelekta attīstību, svarīga ir sabiedrības izglītošana un izpratnes veicināšana par mākslīgā intelekta tehnoloģijām, to radīto ietekmi, ieguvumiem un riskiem, kā arī par to ietekmi uz ētikas principiem un cilvēktiesībām. Tas ir priekšnoteikums turpmākai rīcībai, tai skaitā, lai tiktu pieņemts jauns mākslīgā intelekta regulējums, kas nosaka skaidrus ierobežojumus, aizsardzības garantijas un atbildības mehānismus, kas ir balstīti un aizsargā cilvēktiesības, tiesiskumu un demokrātiju.

Summary

The Role of Human Rights in the Age of Artificial Intelligence. Privacy, Data Protection and Regulation for Preventing Mass Surveillance

The monograph "The Role of Human Rights in the Age of Artificial Intelligence. Privacy, Data Protection and Regulation for Preventing Mass Surveillance" is the first scientific work in Latvia to analyse and explore the legal and human rights implications of artificial intelligence (AI).

AI is a technology undergoing rapid development and has become one of the most powerful drivers of social transformation. AI can bring great benefits in many areas, such as health care, education, culture, employment, transportation, environment, safety and national security and provide opportunities for economic, social, scientific and cultural development. At the same time, AI raises many challenges in all those areas as well as presenting serious ethical, legal and social issues. One of the most serious concerns is AI-based surveillance technologies that pose significant threats to human rights, the rule of law and democracy.

AI-driven surveillance technologies, such as facial recognition, emotional recognition and other biometric technologies, automated decision making and predictive analytics tools have been rapidly introduced in Europe and worldwide. A growing number of states is deploying AI technologies for surveillance purposes – facial recognition technology, smart city platforms, predictive policing, and automated border control systems, which are increasingly used by law enforcement authorities mainly for national security and public safety purposes. More than half of the world's advanced democracies employ artificial intelligence technologies.[719]

The use of facial recognition technology is growing rapidly worldwide both in public institutions and the private sector and it has come under the spotlight and faced major criticism. This technology is increasingly used by the police and other law enforcement authorities, often secretly and without control, a practice that is also present in many European countries, such as France, Germany, Spain, the Netherlands and the United Kingdom. It is also introduced by other public authorities and private companies to carry out surveillance at work, in schools, supermarkets, airports, sports events, and so on.

719 Feldstein, S. (2019). The Global Expansion of AI surveillance. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

International organisations, national legislators and supervisory authorities, non-governmental organizations, human rights defenders and academics are discussing how to regulate this technology and whether certain uses of AI surveillance technology should be prohibited. In 2019, San Francisco was the first US city to ban the use of facial recognition technology by government and law enforcement authorities, soon followed by Oakland, Boston, Minneapolis and other US cities.[720]

In Europe, an intense debate is ongoing about regulating and limiting the use of facial recognition technology. The Council of Europe has called for specific rules concerning biometric processing by facial recognition technologies for law enforcement purposes as well as to strictly limit or prohibit certain uses of these technologies.[721] The European Union (EU) considers regulation of facial recognition technologies as part of an initiative to create an ethical and legal framework for trustworthy AI. The European Commission's White Paper on Artificial Intelligence, published in 2020, emphasizes that the use and gathering of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks to human dignity, autonomy, the right to privacy and other fundamental rights.[722] On 21 April 2021, the European Commission proposed a new Regulation for Artificial Intelligence – known as the AI Act – that is the first initiative in the world that provides a legal framework for AI.[723] The new proposal acknowledges that some AI practices – including social scoring and the use of "real-time" remote biometric

720 Ravani, S. (17 July, 2019). Oakland bans use of facial recognition technology, citing bias concerns. *San Francisco Chronicle.* https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php; Lyons, K. (13 February, 2021) Minneapolis prohibits use of facial recognition software by its police department. *The Verge*. https://www.theverge.com/2021/2/13/22281523/minneapolis-prohibits-facial-recognition-software-police-privacy.

721 Council of Europe. (2021). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). Guidelines on Facial Recognition. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

722 European Commission. (2020). White Paper. On Artificial Intelligence – A European approach to excellence and trust. https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. See also European Parliament. (2020). Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies. https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html.

723 European Commission. (2021). Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

identification systems in publicly accessible spaces for law enforcement – should be prohibited, though at the same time this prohibition is subject to broad exceptions. These provisions have been criticised by the European Data Protection Supervisor and the European Data Protection Board, which have issued a joint statement calling for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces.[724]

Facial recognition technology is also attracting the attention of courts and national data protection authorities. The Swedish and French data protection authorities as well as a French court have issued decisions finding that use of facial recognition technology in schools violates the General Data Protection Regulation (the GDPR)[725].[726] The Swedish data protection authority has also found that the Swedish police authority has processed personal data in breach of data protection rules when using Clearview AI to identify individuals.[727]

The use of facial recognition technology and other forms of biometric mass surveillance in public places is increasingly opposed by civil society. In 2020, EDRi – the European network defending digital rights and freedoms – together with a wide range of civil society organisations launched the "Reclaim your face" campaign, accompanied by the European Citizens' Initiative in 2021, urging the European Commission to strictly regulate the use of biometric technologies and in particular to prohibit, in law and in practice, indiscriminate or arbitrarily-targeted uses of biometrics which can lead to unlawful mass surveillance in order to avoid undue interference with fundamental rights.[728]

724 EDPB, EDPS. (2021). EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en.

725 European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OV L* 119.

726 EDPB. (22 August, 2019). Facial recognition in school renders Sweden's first GDPR fine. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en; CNIL. (29 Octobre 2019). Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position. https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.

727 EDPB. (21 February, 2021). Swedish DPA: Police unlawfully used facial recognition app. https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_lv.

728 EDRi. (17 February, 2021). New ECI calls Europeans to stand together for a future free from harmful biometric mass surveillance. https://edri.org/our-work/new-eci-ban-biometric-mass-surveillance/. See also EDRi. (12 January, 2021). Re: Open letter: Civil society call for the introduction of red lines in the upcoming European Commission proposal on Artificial Intelligence. https://edri.org/wp-content/uploads/2021/01/EDRi-open-letter-AI-red-lines.pdf.

Besides facial recognition, other AI surveillance technologies, which analyse emotions and behaviour and are used for prediction and profiling, raise major concerns about their impact on human rights, democratic values and the rule of law.[729] As the global *biometrics* and emotional recognition market *grows,* there is a trend to use these technologies by law enforcement authorities across European countries lacking transparency, supervision and public involvement. The EU High-Level Expert Group on Artificial Intelligence (AI HLEG) has stressed that identifying and tracking individuals using biometric data, such as lie detection and personality assessment through micro expressions, and automatic voice detection, raises major AI-related concerns of both a legal and an ethical nature.[730] Another great concern is a growing reliance on AI-driven data analytics and predictive tools by police and law enforcement authorities in order to prevent and control crime.[731]

There has been a long and wide-ranging debate about the extent to which a state can use digital surveillance methods of data collection and analysis to carry out surveillance in order to protect such public interests as national security and public safety. Growing security threats have expanded mass surveillance practices all around the world. Edward Snowden's revelations on the US secret mass electronic surveillance program of global telecommunication and data flows of both US and other countries' citizens on a previously unimaginable scale introduced after the 9/11 terrorist attacks triggered global concerns about the impact on human rights of mass surveillance practice by intelligence and law enforcement agencies, in particular on the right to privacy and data protection, as well as lack of regulation, transparency and effective safeguards.[732]

Extensive mass surveillance measures in the name of national security have been introduced not only in the US but also in Europe at both EU and national levels. The European Court of Justice (the CJEU) and the European Court of Human Rights (the ECtHR) play a key role in limiting mass surveillance practices

729 See, e.g., Mcstay, A. (2020). Emotional AI, Soft Biometrics and The Surveillance of Emotional Life: An Unusual Consensus on Privacy, Big Data & Society.

730 AI HLEG. (2019). Ethics Guidelines for Trustworthy AI. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

731 See, e.g., McDaniel, J. L. M., Pease, K. G. (2021). Introduction. In: McDaniel, J. L. M., Pease, K. G. (eds.), *Predictive Policing and Artificial Intelligence*. Routledge, pp. 1–38; van Brakel, R. E. Rethinking predictive policing: Towards a holistic framework of democratic algorithmic surveillance. In: Schuilenburg, M. & Peeters, R. (eds.), *Algorithmic Societies: Power, Knowledge and Technology in the Age of Algorithms*. Routledge, pp. 104–118.

732 See, e.g., OHCHR. (2014). The right to privacy in the digital age, UN Doc. A/HRC/27/37.

as well as promoting and protecting compliance with the right to privacy, data protection and other human rights in the context of mass surveillance.[733]

As an urgent counter-terrorism measure in response to the terrorist attacks in Madrid in 2004 and in London in 2005, the EU Data Retention Directive[734] was swiftly adopted in 2006, despite many concerns about its non-compliance with fundamental rights. In 2014, the CJEU judgment in the *Digital Rights Ireland* case annulled the directive, recognizing that it constitutes an unjustified interference with fundamental rights by requiring EU Member States to oblige telecommunications and internet service providers to retain certain categories of non-content data and to make it available on request to law enforcement authorities for the purposes of investigation, detection and prosecution of serious crime and terrorism.[735] The CJEU has also adopted a number of judgments in response to US mass surveillance practice. It adopted two judgments – in 2015 in *Schrems* I[736], and in 2020 in *Schrems* II[737] – twice annulling European Commission decisions on the adequacy of the level of protection for data transfers from the EU to the US. The ECtHR has been resolving many cases about compliance of national mass surveillance measures with human rights, seeking to find a balance between a person's right to privacy and data protection, on the one hand, and national security and national security interests, on the other hand.[738] The extensive case-law of both courts shows that cancellation of mass surveillance measures introduced for security purposes at both EU and national levels is very difficult and often only possible after lengthy court proceedings.

Alongside the threat of terrorism and security, the Covid-19 crisis caused an even greater flood of new surveillance technologies. To combat the spread of the pandemic, countries around the world have rapidly introduced digital

733 See, e.g., Nesterova, I. (2019). Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards. In: *How International Law Works in Times of Crisis*. Ulrich, G., Ziemele, I. (eds.), Oxford University Press, pp. 109–125.

734 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105.

735 Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* ECLI:EU:C:2014:238.

736 Case C-362/14, *Maximillian Schrems v Data Protection Commissioner,* ECLI:EU:C:2015:650.

737 Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems,* ECLI:EU:C:2020:559

738 See, e.g., European Court of Human Rights. (2020). Guide on Article 8 of the Convention – Right to respect for private and family life. Available: https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

surveillance technologies, ranging from health apps, wearable bracelets, contact tracking and other mobile apps, and digital certificates, to drones and facial recognition technologies.[739] These experiments have significantly shaken human rights, raising new questions about the extent to which privacy, data protection and other human rights can be restricted to ensure public health and safety as well as ways to balance individual and collective interests. Exceptional circumstances do not cancel the requirement to respect human rights.

It is crucial to address the legal, ethical and social issues related to the use of AI and other surveillance technologies in a timely manner. These technologies have a new kind of impact on human rights; they significantly enhance public control based on goals and values that may contradict the values of a democratic society. China's social scoring and so-called 'social credit' system is the most dramatic example.[740]

AI surveillance technologies are different from previous forms of digital surveillance. AI offers new possibilities for data collection, processing and analysis, allows observation to be carried out on a much wider scale and in a more detailed and precise way, thus significantly facilitating the use of surveillance measures. Use of these technologies poses new types of specific risks. They pose a serious threat to the right to privacy and data protection, human dignity and non-discrimination, freedom of expression and peaceful assembly, and to other human rights and freedoms. Moreover, they have a wider impact on the rule of law and democracy.[741] AI significantly increases the scale of mass surveillance by the state and large technology companies and increases power inequalities. Shoshana Zuboff points out that surveillance capitalism has disastrous consequences for democracy and freedom, as it has amassed unprecedented concentrations of knowledge and power with hardly any interference from laws and regulations. This asymmetry of knowledge and power raises new forms of social inequality, and allows shaping of behaviour by individuals and populations in

739 Couch, D. L., Priscilla, R., and Komesaroff, P. A. (2020). COVID-19 – Extending Surveillance and the Panopticon. *Journal of Bioethical Inquiry.*

740 Carney, M. (17 September, 2018). Leave no dark corner. *ABC*. http://mobile.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278?pfmredir=sm&sf197878142=1&smid=Page:%20ABC%20Australia-Facebook_Organic&WT.tsrc=Facebook_Organic.

741 See, e.g., Council of Europe, CAHAI Secretariat. (2020). Towards regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law. https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a.

ways that are inherently antidemocratic.[742] Although this book focuses on state mass surveillance, with commercial surveillance beyond its scope, nevertheless the challenges posed by commercial surveillance, particularly the algorithms of social media platforms that influence and manipulate user opinion, social and political behaviour, are equally important and would deserve a separate study.

In order to ensure that the use of AI is in line with human rights and does not violate them, it is crucial to assess the existing regulatory framework as well as to develop new strong regulation setting clear limits on when AI can and cannot be used and requiring effective safeguards and supervision mechanisms. There is an urgent need to set limitations on AI surveillance measures in order to protect human rights and democratic values. Regulation is an essential tool in order to ensure accountable and human-centred AI, and to prevent the potential harm it can cause.

In the last few years, international organizations – notably the Council of Europe[743], the United Nations Educational, Scientific and Cultural Organization (UNESCO)[744], the Organization for Economic Co-operation and Development (OECD)[745], the EU[746], as well as many non-governmental, professional and other organizations[747] – have been rapidly developing ethical guidelines defining the values, principles for development, implementation and use of AI. However, there is a growing emphasis on the need for regulation to go beyond ethical

742 Naughton, J. (20 January 2019). 'The goal is to automate us': welcome to the age of surveillance capitalism. *The Guardian.* https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook. See also Zuboff, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the new Frontier of Power*. Profile Books.

743 Council of Europe. (2020). Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the human rights impacts of algorithmic systems. Adopted 08.04.2020. https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

744 UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137.

745 OECD. (2019). Recommendation of the Council on Artificial Intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

746 AI HLEG (2019), Ethics Guidelines for Trustworthy AI.

747 See, e.g., IEEE. (2019). Ethically Aligned Design. First Edition: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems. https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf?utm_medium=undefined&utm_source=undefined&utm_campaign=undefined&utm_content=undefined&utm_term=undefined; Fjeld, J., Achten, N., Hilligoss, H., et al. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Berkman Klein Center Research Publication No. 2020-1. https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y.

norms, and to establish legally binding requirements at both the international and national level, and to implement effective practical mechanisms to put AI ethical principles into practice. Both international organizations and countries around the globe are currently actively looking for possible ways to regulate AI.

At the same time, the existing legal framework – particularly human rights and data protection rules – are already applicable to AI. Human dignity, the right to privacy and data protection, the principle of non-discrimination, freedom of expression and assembly, and other human rights and freedoms are of particular importance and are applicable to AI surveillance technologies. These rights and freedoms can help to redefine red lines in terms of their use. The requirements on collection and use of personal data and accountability measures that are set in the data protection rules – particularly in the GDPR and the Law Enforcement Directive[748] – are also critical in relation to the development, deployment and use of AI surveillance technologies.

The book demonstrates that human rights and data protection standards provide the most secure basis for further development of AI regulation, and that a clear AI legal framework needs to be introduced by further developing international human rights and European data protection rules, building upon the existing case-law of the CJEU and the ECtHR. In addition, clear limitations need to be set on certain uses of AI surveillance technologies. It is therefore necessary to fully assess the effectiveness and shortcomings of the existing legal framework and then consider the need for a new framework. New legislation should only be adopted once the issue has been properly understood, following public debate, and once it has been established that existing laws are not sufficient to address the issues identified.

In this book, a coprehensive approach is taken to analyse and explore the legal and human rights implications of AI as well as surveillance technologies, their risks and threats, providing concrete recommendations for the development of regulation and policy at both international and national levels.

This book aims to examine the human rights implications of AI surveillance technologies and evaluate existing and future regulation in order to prevent the risks and threats posed by these technologies. More specifically, the author explores the development of AI mass surveillance technologies and their use by law enforcement authorities in Europe and beyond. The author proceeds to

748 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L* 119, 04.05.2016.

analyse the impact of these technologies on human rights as well as the wider effect on society and fundamental democratic principles. Further on, the author evaluates how the rights to privacy and data protection, the conditions for their limitations developed in case-law and European data protection standards apply to AI surveillance technologies, as well as examining AI regulation at both international and EU levels. Lastly, the research offers recommendations for development of a legal and regulatory framework for AI surveillance technologies and the safeguards and mechanisms that should be introduced to prevent threats and risks and ensure responsible and human-centric use of AI surveillance technologies.

Analysis of human rights, data protection and AI regulatory and legal framework, guidelines and other documents developed and adopted by the UN, UNESCO, the Council of Europe, the OECD and EU institutions, plays an important role in the study. Documents developed by national institutions and data protection institutions and other public institutions, non-governmental organizations, and international AI expert groups have also been used in the work. In addition, the book extensively analyses and compares the case-law of the ECtHR and the CJEU. Although the research mainly analyses legal aspects of AI surveillance technologies, the study makes extensive use of an interdisciplinary approach. In order to understand AI technologies and reveal not only their legal, but also their social and ethical implications as well as their impact on society and democracy, a wide range of research was examined: books, scientific articles, reports and other documents in sociology, ethics, philosophy, politics, technology and other fields.

The book is organized in seven chapters. This summary will briefly describe the topics examined in each chapter, the main conclusions, proposals and recommendations, which are mostly provided in the last two chapters, that is, in Chapter 6, where proposals for improving data protection rules are laid down and in Chapter 7, which summarises the analyses and offers policy recommendations for the further development of human rights-based AI.

Chapter 1, AI and state surveillance, introduces the topic and explains AI and surveillance from a social and technological point of view, revealing how the development of new technologies from big data to AI has influenced and facilitated mass surveillance. First of all, technological concepts are explained, that is, AI (definition and subdomains), the relation of AI to big data, personal data and the concept of profiling. It goes on to explain the concept of surveillance, the imbalance of power as a feature of surveillance, the distinction between mass surveillance and targeted surveillance as well as examining how national security and public safety have long been fertile ground for introducing various types of mass surveillance measures by law enforcement and intelligence agencies.

The chapter then explores how AI has significantly increased surveillance practices and examines specific AI surveillance technologies and methods – facial recognition technology, emotion recognition technology and predictive policing – and, finally, reveals how the Covid-19 crisis has contributed to the use of digital surveillance technologies.

Chapter 2 examines the impact of AI surveillance measures on human rights. The chapter examines human rights that are most impacted by those measures: – human dignity; – the right to privacy and data protection; – the principle of non-discrimination, – the rights of the child; – the rights to an effective remedy and to a fair trial; – freedom of expression; – freedom of assembly and association. The book examines how these rights are regulated in international and European human rights instruments, in particular the European Convention on Human Rights (the ECHR), the Charter of Fundamental Rights of the European Union (the Charter) and the Constitution of the Republic of Latvia[749], revealing how these rights are challenged by AI mass surveillance measures. The chapter goes on to explore the wider impact of these technologies on society, the rule of law and democratic values.

Human dignity constitutes the foundation of all human rights and fundamental freedoms and is essential for the development, deployment and use of AI systems. Every human being possesses an intrinsic value and should be treated with respect; this also applies with regard to use of AI systems. Human dignity should be the counterweight to mass surveillance practices and asymmetry of power. Likewise, AI surveillance practices touching the essence of the right to human dignity should be prohibited.

The right to privacy includes a wide range of elements. Besides personal or general privacy, it also encompasses physical, psychological or moral integrity, and the identity and autonomy of the person. AI surveillance technologies have a profound impact on all these elements. Use of facial recognition technology involves acquisition, comparison and storage of biometric facial images in IT systems. Each of these actions constitutes an interference with the right to privacy and the right to protection of personal data. Other forms of AI biometric recognition, which include analysing and predicting our behaviour and emotions through facial expressions, tone of voice, gait, and heart rate, further affect our psychological integrity, deeply interfere with our personal sphere and severely limit our ability to freely express our personality and autonomy. It is important to remember that very often no scientific evidence is available on the claimed abilities of AI technologies; for example, there is no proof that a person's inner

749 The Constitution of the Republic of Latvia. Adopted on 15. February 1922 (came into force on 7 November 1922). *Latvijas Vēstnesis*, 01.07.1993., No 43.

emotions can be accurately "read" from facial expressions, heart rate or tone of voice.

Use of AI surveillance systems can lead to discrimination. Studies have shown that AI algorithms in facial recognition technology work differently depending on the age, gender, or ethnicity of the person being identified. As a result, members of these groups may be more likely to be discriminated against, for instance more often being unwarrantedly stopped or detained by police. The use of such technologies could be used to control and track the most marginalized communities and enhance discrimination against certain ethnic groups. AI surveillance systems can have a particularly negative impact on vulnerable groups such as children and the elderly, especially as the accuracy of face recognition is significantly lower for children.

Children and their rights are significantly affected when they are directly engaged with AI surveillance activities, but also in the case of indirect engagement through tools such as surveillance cameras and predictive modelling. The well-being and full development of children are limited when their freedom and autonomy are constantly restricted by AI systems, including surveillance systems.[750]

AI surveillance technologies can also restrict individuals' right to a fair trial and effective remedies. Facial recognition systems often make mistakes in determining whether a person is dangerous. This, in turn, can lead to unjustified detention, accusation and even conviction of innocent people. The use of AI systems in law enforcement may raise concerns about fair trial standards, in particular the presumption of innocence, the right to be informed promptly of the cause and nature of accusation, the right to a fair trial and the right to defend oneself.

The use of surveillance measures such as facial recognition technology in public places may restrict a person's right to freely express their views and opinions, as well as freedom of assembly and association. Surveillance of public places with facial recognition technologies can have a chilling effect and can make people change their behaviour and impact their willingness to attend demonstrations or engage in public activism.

In addition to posing risks to human rights, AI surveillance technologies can also endanger the rule of law and democracy. The rights to freedom of expression, freedom of assembly and association are essential in a democratic society. The use of new technologies, which can disproportionately restrict and violate those freedoms, also threatens the very foundations of a democratic society.

750 UNICEF. (2020). Policy guidance on AI for children. Draft 1.0. https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf.

The chapter also examines the obligation to respect human rights during a crisis situation, stressing that even in such emergencies as Covid-19 citizens do not have to choose between respecting human rights and protecting such interests as public safety and health. Restrictions on human rights must still be legitimate, necessary and proportionate in terms of achieving the particular aim, as well as limited in time.

Chapter 3 analyses the importance of privacy. Mass surveillance exercises a significant impact on the right to privacy; moreover, many attempts are being made to devalue privacy – and are being widely criticized. The chapter reveals why privacy should be protected and outlines its value and meaning, before going on to examine various theories and analysing the rationale and role of the right to privacy in limiting AI mass surveillance measures. It reveals that the right to privacy has been recognized as: – the right to be left alone, – the right to control information about oneself; – an essential aspect of human dignity, autonomy and free will; – protection against abuse of power. The chapter looks at the right to privacy in international human rights treaties and explores how this right helps to protect other human rights, for example, freedom of expression and assembly. It also reveals how academics increasingly acknowledge the importance of group privacy, which protects against pervasive mass surveillance and asymmetry of power. Further, the importance of rising awareness about privacy has been highlighted, spearheaded by a number of individuals, in particular Edward Snowden, Maximilian Schrems as well as fostered through *Cambridge Analytica* and other scandalous cases of illegal use of data by large technology companies. The end of the chapter brings to attention the fact that the Covid-19 crisis can also lead to a crisis of privacy. There is an urgent need for a new regulatory framework to prevent threats to privacy and other human rights.

Chapter 4 contains an overview on the development of data protection law and the first initiatives to regulate AI. The chapter begins with a brief introduction on how data protection law marks the beginning of information and communication technology rules trying to balance the different public and private interests. After that, it introduces international initiatives and the EU path from the gold standard for data protection to AI regulation.

Section 1 examines how international organisations – the Council of Europe, the OECD, the UN, UNESCO – have developed data protection law, how these organisations have engaged in the debate about the impact of mass surveillance on human rights as well as exploring their first actions towards creating AI regulation.

International organizations, especially the Council of Europe and the UN, have for a long time been calling for revision of international as well as national rules and for strengthening data protection standards in order to provide effective safeguards against mass digital surveillance measures. The recommendations

provided by those organisations are largely applicable to AI surveillance measures. Many earlier proposals regarding regulation of digital surveillance can be found in AI ethical guidelines, such as requirements to respect the principles of proportionality, transparency and accountability.

Section 2 examines the development of EU data protection law. Firstly, it is noted that the EU is founded on respect for human rights, freedom, democracy and the rule of law, and that the importance of human rights has greatly increased in EU legislation. The EU's fundamental rights-based approach, which underpins the development of data protection law, should also form the basis for the further development of AI regulation.

This is followed by an examination of EU data protection reform and the GDPR as well as specific legal instruments on data protection, especially the Law Enforcement Directive. The author draws attention to the fact that the EU data protection rules do not constitute a fully uniform system. Both the EU and Member States should review legal acts adopted before the GDPR and assess the necessity for new specific data protection rules, including in relation to AI application in different sectors. The data protection rules will be strongly influenced by the regulatory framework that is being developed for Europe's digital future, including AI regulation.

Finally, the author examines the development of AI regulation in the EU. To date, discussions on AI regulation are fundamentally based on the EU's digital single market agenda. While these policy discussions may refer to the need to consider law enforcement and criminal law specificities, they often lack detailed review and fail to take into account specific applicable rules, in particular restrictions and derogations.[751] The chapter reveals that both international organisations and the EU are rapidly developing new regulation, effective safeguards and accountability mechanisms for AI systems, including new provisions for preventing and limiting the use of AI surveillance technologies.

Chapter 5 analyses the jurisprudence of the CJEU and the ECtHR on interference with the right to privacy and data protection through mass surveillance.

Section 1 explains the conditions for limiting the right to privacy and other rights and freedoms set out in the ECHR and the Charter. Section 2 analyses the most important cases: the case-law of the ECtHR examining whether national surveillance measures comply with human rights as well as the case-law of

751 Gonzelez Fuster, G. (2020). Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf. See also Drechsler, L. (2021). Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context. *International Data Privacy Law*, 11(2), pp. 182–195. https://doi.org/10.1093/idpl/ipaa019

the CJEU on mass surveillance cases related to the validity or interpretation of EU law. Section 3 examines the four essential guarantees based on the jurisprudence of the CJEU and the ECHR:

- clear, precise and accessible rules;
- proportionality and necessity;
- independent oversight mechanism; and
- effective remedies.[752]

The case-law of both courts reveals that mass surveillance measures constitute an intrusion into privacy and data protection. It is essential to have clear, precise and accessible rules governing the scope and application of these measures. The rules should provide minimum safeguards against arbitrary interference and the risk of abuse that counterbalance secrecy and allow individuals to foresee when the authorities are likely to apply these measures, thus allowing them to adjust their behaviour.

On the principle of proportionality, the ECtHR and the CJEU have emphasized that one of the crucial requirements is to ensure that interference with the right to privacy and data protection through surveillance measures does not exceed the limits of what is strictly necessary. It is of great importance to apply this condition also to AI surveillance measures. Prior to the introduction of surveillance measures, there must be evidence regarding their effectiveness in achieving the particular public interest objective, while the measures chosen should be the least restrictive means for achieving that objective. Many examples show that in practice facial recognition systems are often introduced without considering whether they are "strictly" or "absolutely" necessary and proportionate, furthermore, that they are used secretly without informing individuals and the public. Such practices not only violate the right to privacy, but are also contrary to the rule of law and can have a negative effect on democracy.

The extensive jurisprudence of European supranational courts on mass surveillance clearly shows the importance of human rights organizations and activists in promoting effective safeguards against mass surveillance measures. Many non-governmental organisation and privacy rights activists have initiated strategic cases to protect the interests of society and each individual from being subjected to disproportionate mass surveillance measures. Given that each individual may have limited opportunities to defend their rights, mechanisms for protection of collective interests as perceived by individuals should be strengthened.

752 See EDPB. (2020). Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en.

Chapter 6 analyses data protection requirements and their applications to AI surveillance technologies, in particular facial recognition technology, and the challenges that AI presents to data protection rules. The chapter analyses and compares the requirements set out in EU data protection law – the Law Enforcement Directive that applies to law enforcement authorities and the GDPR, as well as the Council of Europe's Convention108+[753].

Section 1 explains the meaning of personal data and biometric data, pointing out that facial images are considered to be biometric data if they allow unique identification or authentication of a natural person. It discusses the different uses of facial recognition technology, for instance authentication and identification, which is seen as more dangerous, and profiling of individuals based on their personal characteristics. The author argues that suggestions by legal scientists to recognize that new information about a person inferred by algorithmic models can be regarded as personal data have to be supported.[754] It also points out that "real-time" remote facial recognition technology in publicly accessible places poses an even higher risk post-event use of these systems as the number of false matches increases in uncontrolled public places.

Section 2 examines the principles of personal data processing that lie at the heart of all other data protection requirements. First examined is the principle of lawfulness, which requires a legal basis for processing personal data and allows processing of special categories of data only in certain exceptional and limited circumstances. Public authorities are allowed to process biometric data where this is strictly necessary for reasons of substantial public interests and where they are authorized by law, which must be proportionate, respect the essence of fundamental rights and provide appropriate safeguards. While these are important requirements, countries are left with a wide discretion to decide when the use of facial recognition and other AI surveillance technologies in the public sector is "absolutely necessary and proportionate" to protect substantial public interests.

As for the principle of purpose limitation, there is a risk that personal data – facial images – that are used to train or develop facial recognition technology were originally collected for a different purpose and a legal basis for the new purpose is lacking. It must be ensured that images available in digital format – for example, from social media – could not be processed to obtain biometric

753 Council of Europe. (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data – Consolidated text. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

754 Sartor, G. (2020). The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence. European Parliament. http://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

templates or integrated into biometric systems without a specific legal basis for the new processing when those images were originally taken for other purposes.

Principles of fairness and transparency require that individuals are informed about use of surveillance technology and its purposes, the existence of automated decision-making as well as to provide meaningful information on its logic and expected consequences. At the same time, it is unclear what the logic and consequences of an automated decision mean, as there is a conflict between the need to provide concise and easily understandable information, on the one hand, and accurate and in-depth information, on the other. Likewise, the principle of fairness is linked to concerns about fairness and non-discrimination in automated decision making. Transparency may also require access to data, in particular to the AI system training set, in order to identify possible causes of unfairness or bias resulting from insufficient or biased data or the training algorithm. This is especially important where the algorithmic model is not transparent, as a result of which it is not possible to detect possible mistakes or cases of discrimination. While systematic transparency in law enforcement may hinder crime prevention or the effectiveness of public criminal investigations, at the same time there is a need for some transparency in order to inform individuals about the risks, rules, guarantees and rights regarding processing of their personal data and how to exercise and defend their rights.

The data minimization principle requires that the principle of proportionality be applied in order to evaluate whether it is possible to minimize the amount of data or reduce their "personality" by using appropriate technical means.

The principle of accuracy – requiring that personal data are accurate and, where necessary, kept up to date – also raises challenges with regard to AI surveillance technologies. One of the biggest concerns regarding these technologies is that they are not sufficiently accurate. Moreover, erroneous results are related to data quality and accuracy of data processing. Additionally, members of a particular group may suffer from prejudice if that group is not represented proportionally in the training data, since AI models trained on such data will produce biased predictions towards the underrepresented group.

As for the data security principle, it is emphasized that facial recognition and other biometric technologies pose significant security risks that are difficult or even impossible to predict. Biometric data such as fingerprints and facial images cannot be replaced, unlike other forms of authentication, such as passwords. Thus, biometric data security breaches can have particularly serious consequences for data subjects, as unauthorized disclosure of such sensitive data cannot be corrected. Strict security measures should be implemented at both technical and organizational levels at all stages of processing to protect facial recognition data and image sets against data loss and unauthorized access or use.

In accordance with the principle of accountability, public and private entities must be able to demonstrate compliance of AI systems that rely on processing of personal data with all data protection requirements. They are required to implement appropriate technical and organizational measures, for instance transparency policies and reports, prior impact and accuracy assessment, and integrate data protection into the design and architecture of AI systems.

Section 3 analyses automated decision making and the human oversight requirement. Facial recognition technology algorithms never provide a final result, but only probabilities. Although the accuracy of this technology is increasing, there is always a certain level of error. Decisions that are based solely on this technology – like any other automated processing which produces an adverse legal effect concerning the data subject or significantly affects them – should be prohibited.

Data protection rules in exceptional cases accept such decisions, including those based on biometric data, if they are authorized by law that provides suitable measures to safeguard the rights and freedoms of the data subject, including the right to obtain human intervention on the part of the controller. However, their use should be strictly limited and there should be supervision and impact assessment, for example evaluating whether such decisions do not discriminate against persons on the basis of underrepresented categories before they can be implemented.

The safeguards to be applied in the case of automated decision-making, in particular when biometric data are processed, include the right to obtain human intervention, for the data subject to express their point of view and to contest the decision, the right to be informed of the existence of automated decision-making, including profiling, to obtain meaningful information about the logic involved as well as the significance and expected consequences of such processing for the data subject.

Human oversight – the new requirement introduced in the proposal for an AI Act – is closely linked to the data protection requirement for the right to obtain human intervention in a case of automated decision-making. Human oversight is a vital requirement for use of facial recognition and other AI surveillance technologies and must be ensured in all cases. However, this requirement is not clear. It could be incorrectly implemented as simple validation of all system results, making it fully automated. Opposite cases, when people review and potentially override the system's results, could also raise concerns, since in practice people might tend to override the results of algorithms if the results are in line with their stereotypes, thereby putting minority groups at a disadvantage.[755]

755 Sartor (2020), The Impact of the General Data Protection Regulation ..

Section 4 examines data subject rights and emphasizes that, since facial recognition and other AI surveillance systems are based on processing of personal data, data subjects must be guaranteed all data subject rights: the right to information, which lies at the heart of the principle of transparency, the right not to be the subject of automated decisions, the right of access, the right to object, rectification and erasure of data as well as the right to effective protection of rights.

People often do not know that their facial images are recorded and processed in a database for comparison. If they are not informed and aware of processing, they cannot exercise other rights.

In addition to the right to information, the right to access is also important with regard to AI surveillance measures. Both rights are linked and allow exercise of the right to an effective remedy. Although the data subject's right of access is not the same as the right of access to files or documents, both rights derive from the requirement of good administration and the obligation of any public authority to state reasons for its decisions.

One of the challenges is how to ensure the accuracy of facial recognition systems. In the event of a false match of facial images, data subjects may request corrections to avoid the system re-establishing a false match in the future.

Another difficult question is whether the obligation to delete personal data also includes inferred personal data or inferred group data, such as a trained algorithmic model.

Although the rights of data subjects, including the right to information, the right to access data and the right to delete data can be restricted, for instance arising from obligations of law enforcement authorities to work with a certain degree of confidentiality and secrecy, in order to ensure the effectiveness of their work. However, these restrictions must be laid down by law and must be necessary and proportionate in a democratic society as well as compensated by other safeguards, such as oversight by independent authorities, public supervision, and so on. In this regard, the right to an effective remedy is of particular importance to prevent arbitrary and unlawful data processing. In the event of a restriction, law enforcement authorities must inform individuals, *inter alia*, of the measures taken if the notification is no longer likely to jeopardize their investigations, their right to complain to the supervisory authorities and their right to an effective judicial remedy. This obligation also applies to data used for facial recognition and other surveillance technologies. People may want to dispute that their facial image is on a 'watch list' in case this was done in a non-transparent way and without their consent, or seek redress for a false positive match that has had negative consequences for them such as unlawful detention or arrest as well as claim compensation for any damage caused.

Section 5 examines data protection impact assessment as one of the most important AI accountability tools. The data protection rules require a data protection impact assessment before implementing facial recognition and other biometric surveillance technologies and also require prior consultation with data protection authorities. These requirements play a significant role in preventing implementation of controversial new surveillance technologies that pose high risks to fundamental rights.

Section 6 explores data protection standards for Covid-19 contact tracking apps that have been developed by many international and European organizations. Many of the requirements that were identified during discussions – such as effectiveness, transparency, impact assessment, voluntariness, independent monitoring – are also of particular importance with regard to AI surveillance technologies. The speed with which a wide range of stakeholders – scientists, technology companies, civil society organizations, international organizations – were involved and collaborated to develop standards for the implementation and evaluation of these apps could serve as a good example of how to evaluate legal compliance of other new technologies.

Chapter 7 is the final chapter, summarizing the discussion and the main findings and providing recommendations for further development of AI regulation based on human rights. It also advises what governance mechanisms and safeguards need to be put in place to ensure responsible and trustworthy use of AI systems and to prevent risks and threats to human rights, democracy and the rule of law.

Section 1 "beyond ethical principles" emphasizes that discussions on regulation of AI have so far mainly focused on ethical principles and mostly offer general recommendations and suggestions, rather than how to develop effective enforcement mechanisms and a framework for their practical implementation. Therefore, regulation needs to go further. Agreeing on common and internationally recognized moral norms is essential, as they provide ideals, inspire action, and mark a clearer direction for AI development that will serve and bring benefits to humanity and society. However, AI regulation cannot be based solely on AI ethical principles. Methods and tools must be identified to put ethical values and principles into practice. In this regard, legal requirements play a crucial role. It is necessary to define a set of harmonized rules that constitute the minimum requirements to be met in order for AI systems to be recognized as ethical and legitimate. Human rights lie at the heart of ethical principles, and respect for them in the context of democracy and the rule of law is the most secure way of defining abstract ethical principles and values.

Section 2 further explains that human rights form the cornerstone of AI regulation. International human rights law establishes global standards, that

is, a universal set of rules and minimum standards, based, *inter alia*, on human dignity, autonomy, equality and the rule of law, that determine how people should be treated. These standards and related legal mechanisms create clear legal obligations for states to respect, protect and implement human rights. They also require that persons whose rights have been denied or violated have the right to an effective legal remedy.

Human rights form the basis of AI regulation and play a key role in the further development of the international and EU AI legal framework. This has been emphasized in many AI ethical guidelines developed by international organizations, such as the Council of Europe[756], the EU[757] and UNESCO[758] as well as by academic researchers[759]. There are many advantages to using human rights-based regulation in the context of AI. Over time, a broad human rights protection system has been established at the international, regional and national levels where individuals can seek legal remedies in the case of human rights violations. There is established case-law on how to interpret and apply these remedies in specific situations. Human rights provide a universal language for global issues and they are internationally recognized.

At the same time, there are also challenges to implementing a human rights-based approach to AI. Human rights are more oriented towards states than private actors. They are better suited for reducing significant harm to a small number of people than for preventing harm to the collective interest. AI, including surveillance systems and their effects on human rights and freedoms, is more difficult to challenge individually. At the societal level, joint and coordinated action is needed to protect privacy and autonomy as a public good.[760]

Within the European human rights protection system, a human rights-based AI regulatory framework could be established as a model for the rest of the world. The EU is founded on the values of human dignity, freedom, democracy, the rule of law and respect for human rights. The EU could create a "gold standard" in the form of regulation for a human rights-based AI that would be directly applicable in all Member States, similar to EU data protection rules. The Council of Europe as the continent's leading human rights institution could also develop

756 Council of Europe, CAHAI Secretariat (2020), Towards regulation of AI systems.

757 European Commission (2020), White Paper. On Artificial Intelligence.

758 UNESCO (2022), Recommendation on the Ethics of Artificial Intelligence.

759 Mantelero, A. (2020). Regulating AI within the Human Rights Framework: A Roadmapping Methodology. In: Czech, P., Hesch, L., Lukas, K., Nowak, M., Oberleitner, G. (eds.), *European Yearbook on Human Rights. Interesentia*, pp. 477–502.

760 See Taylor, L., van der Sloot, B., Floridi, L. (2017). Conclusion: What Do We Know About Group Privacy? In: *Group Privacy*, Taylor, L., Floridi, L., van der Sloot, B. (eds.), Cham: Springer International Publishing, pp. 225–37.

a clear framework based on human rights, the rule of law and democratic values by adopting a new legally binding instrument, such as a framework convention. Future legal regulation of AI should further develop human rights norms by clarifying their application to specific use cases. It should be built on existing human rights instruments, but also go beyond them, in order to adapt and contextualize the application of these rights and freedoms and address the shortcomings of legislation created before the AI era.[761]

Section 3 emphasizes the need for new AI regulation. The need for a clear legal framework for AI has been increasingly acknowledged by international organisations, including the EU and the European Council. Although existing legal norms, in particular human rights and data protection law, already regulate AI, this regulation has a number of shortcomings. Firstly, the rights and obligations set out in existing legal instruments are usually formulated broadly or in general terms, and it may be difficult to interpret them in relation to AI systems. Moreover, they clearly do not address some issues related to AI. Secondly, a number of key requirements and safeguards related to protection of human rights, democracy and the rule of law in the AI field are currently not explicitly enshrined in law – for instance human control, supervision, transparency and accountability. Thirdly, current instruments also do not pay enough attention to the steps that developers and deployers of AI systems need to take to ensure the effectiveness of AI systems whenever they may have an impact on human rights, democracy or the rule of law as well as to ensure that they have the necessary competences or professional qualification.

Existing human rights and data protection norms should be adapted to the specificities of the field. A new legal framework for AI could combine adoption of a new general legally binding instrument with sectoral instruments, both legally binding and non-binding, that would address specific sectoral challenges of AI, especially in high-risk areas such as law enforcement.[762] While human rights and data protection legislation lay down important requirements for the development and use of AI surveillance technologies, in particular facial recognition technology, new specific rules need to developed and adopted that would clarify how these existing rules should be applied to surveillance activities for law enforcement purposes.

761 Mantelero (2020), Regulating AI within the Human Rights Framework, pp. 477–502.

762 Council of Europe. (2020). Ad Hoc Committee on Artificial Intelligence (CAHAI) Feasibility Study. https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da.

Section 4 argues that red lines should be drawn on mass surveillance and clearly set in forthcoming AI regulation.[763] AI systems should not be used for mass surveillance. The AI legal framework should include a prohibition on indiscriminate use of facial recognition and other biometric surveillance technologies that could lead to mass surveillance in public or publicly accessible spaces. Law enforcement authorities do not need to carry out mass surveillance in order to ensure citizens' security or safety, as surveillance should always be targeted as well as strictly necessary and proportionate. Facial recognition technology is often used unlawfully and discriminatorily in both public and private sectors. These practices may cause significant harm and violate fundamental rights and democratic principles. A moratorium on targeted use of facial recognition technologies should be introduced. In like manner, this concerns other types of AI technologies posing high risks to fundamental rights, the rule of law and democracy. Their effectiveness and benefit to society should be clearly demonstrated to prevent arbitrary and unlawful use. Emotional recognition systems drawing conclusions and predictions about our behaviours, thoughts and other personal characteristics as well as biometric categorisation systems should likewise be prohibited by law, since the use of such technologies in itself violates human dignity, autonomy and other fundamental rights. Similarly, use of AI-enabled predictive policing methods by law enforcement authorities such as AI systems intended to be used for predicting the occurrence or reoccurrence of criminal offences based on profiling of a natural person or on assessing personality traits and characteristics or past criminal behaviour should not be allowed. AI-enabled social scoring and manipulation or control of human behaviour should be prohibited by law as well, since these practices pose significant threats to fundamental democratic principles and freedoms.

It is important not to miss the crucial moment when international and European organisations, as well as national legislators, are developing AI legal regulation and when it is possible to prohibit uses of AI systems that pose significant risks and threats to human rights, the rule of law and democracy. International organisations are increasingly recognising the importance of introducing clear limitations on certain uses of AI technologies that violate and pose threats to human rights, the rule of law and democracy, at the same time hesitating to propose specific legal provisions. It is of paramount importance to legally

763 See ibid.; EDRi. (17 February, 2021). New ECI calls Europeans to stand together for a future free from harmful biometric mass surveillance. https://edri.org/our-work/new-eci-ban-biometric-mass-surveillance/; Council of Europe. Ad Hoc Committee on Artificial Intelligence (CAHAI). (2020). The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law. Report by Muller C. https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da.

impose clear legal restrictions in the forthcoming AI legal framework at both the international and EU regulation levels. The EU, the Council of Europe as well as other international organisations should gain momentum while there remains a real opportunity to introduce strict restrictions in forthcoming AI regulation. It is not even a question of whether we might want or accept a particular use of AI systems or not. Clear restrictions, prohibitions or a moratorium would not constitute new red lines, but rather ensure recognition of existing ones. It must be acknowledged that use of AI surveillance technologies for mass surveillance already violates our dignity, fundamental rights and freedoms and democratic principles. If the new AI legal framework lacks such prohibitions and restrictions, it will be very hard to prevent mass surveillance measures from becoming the new normal in the decades to come. While discussions are still open, we are obliged to take persuasive steps in order to protect human rights, the rule of law and democracy.

Section 5 argues that impact assessment is one of the main AI accountability mechanisms that has been widely supported by international and European organisations[764], governments[765], academics[766] and other organisations. AI impact assessment can be an important accountability tool to ensure that institutions and companies are aware of – and assess – the risks of AI technologies and evaluate their wider impact on human rights, the rule of law, democracy, as well as social, ethical and other implications. It can also be an effective tool for informing the public and individuals about the use of such AI systems.

However, a risk-based approach to AI regulation is not enough to protect human rights. AI should not be regulated on the basis of risk, but on the basis of human rights. Regulation should not require only institutions and companies themselves to assess the risks of AI surveillance technologies to human rights, society and democracy but rather this should be done by an independent third party, because both public authorities and companies may have an interest in underplaying risks in the development, implementation and use of AI technologies. Although the EU data protection framework already imposes an obligation to assess the impact of AI technologies on individual rights and freedoms, many cases show that this requirement does not effectively prevent introduction of AI surveillance technologies violating data protection rules and human rights law.[767]

764 Council of Europe Commissioner for Human Rights (2019), Unboxing Artificial Intelligence ..

765 Government of Canada, Algorithmic Impact Assessment.

766 Mantelero (2018), AI and Big Data ..; Reisman et al. (2018), Algorithmic Impact Assessments Report.

767 EDPB (21 February, 2021), Swedish DPA ..; EDPB. (22 August, 2019). Facial recognition in school renders Sweden's ..

Human rights are non-negotiable and must be respected regardless of the level of risk.

Section 6 examines independent oversight and public participation as important safeguards to ensure AI accountability. Control by an independent supervisory authority, as well as public oversight, is particularly important for high-risk AI technologies, such as facial recognition and other biometric surveillance technologies. In order to ensure accountable use of AI technologies and to prevent the threats they raise, it is necessary to establish an effective, transparent, inclusive monitoring and independent oversight mechanism.[768] At European level, many proposals have been made to set up an independent supervisory authority to monitor the use of AI systems and its compliance with human rights and other legal requirements. It is also important to recognize the crucial role of existing national authorities, in particular data protection authorities, human rights authorities and ombudsman institutions to ensure effective monitoring of AI systems. National supervisory authorities must be provided with sufficient resources, powers and competences to prevent and assess violations of fundamental rights, and to provide effective support to those whose human rights are affected by AI systems.

Effective monitoring of AI systems requires close cooperation amongst a broad range of relevant stakeholders, including public authorities, private actors, academics and civil society organizations representing the interests of different groups. Public participation with the active engagement of individuals and groups potentially affected should also be included in the impact assessment of controversial AI technologies by involving the individuals and groups these technologies may prospectively affect.[769] When conducting AI impact assessment, supervisory authorities should organise consultations with different stakeholders and experts in various fields, such as computer sciences, data sciences, health and behavioural sciences, social sciences, ethics and law. It is not the police or other law enforcement authorities that are planning to use AI surveillance technologies, but independent supervisory authorities, with the assistance of individuals, groups and other stakeholders, that should evaluate whether the systems should be used and *ex ante* assess the balance between privacy and security interests. Monitoring and independent oversight together with public participation mechanisms are essential to prevent the development, deployment and use of AI surveillance technologies that violate human rights, other legal requirements

768 Council of Europe, CAHAI (2020), Feasibility Study.

769 Ibid.; European Parliament (2020), Report with recommendations to the Commission on a framework ..; Mantelero (2020), Regulating AI within the Human Rights Framework, pp. 477–502.

and democratic values. These mechanisms are essential for meeting people's expectations on acceptable use of AI technologies as well as for identifying and introducing red lines for undesirable and harmful technologies.

Independent monitoring and public participation are the safeguards for a so-called strategic level of supervision. There is also a tactical level of supervision, which sets out the rules that have been adopted for use of the system for certain purposes and defines the requirements to be met in each individual case. An essential requirement for surveillance technology is prior approval or warrant by an independent judge, which can authorize targeted use of surveillance technology for national security purposes. Such a safeguard as an important guarantee against unfair practices and abuses of power also stems from the extensive mass surveillance case-law of the ECtHR and the CJEU.

Section 7 explores transparency and awareness as crucial AI safeguards. Use of AI systems is often hidden or unknown, making it difficult or impossible to assess their impact and monitor their use. If individuals and society are unaware of the use of AI surveillance systems, they cannot know about infringement of their rights and freedoms and ensure their protection. The legal framework should include clear transparency requirements. For example, a legal obligation to publish an impact assessment of AI systems as well as public consultation results reflecting the views of experts and members of the public, particularly regarding high-risk technologies. The requirement for AI developers and deployers to make available information in order to enable the supervisory authority to assess AI systems should also be introduced. The supervisory authority should also educate and raise public awareness of AI implications, risks, threats and accountability requirements.

One proposal that would make a significant contribution to transparency is to establish a register of AI systems.[770] The register could be set up at the national level as well as at the EU level and include information about use of AI systems by public institutions and in high-risk sectors, with uses or purposes including law enforcement, migration, border control, and the judicial sectors in all EU Member States.

Awareness and education are essential to create trust as a precondition for AI systems to be used and accepted. First of all, we need to raise public awareness that will lead to action, that is, call for AI systems that bring benefits to society and do not pose risks and threats to rights and freedoms. Education and awareness-raising are the precondition for individuals to be aware of their values and rights and to be able to protect them.

770 See, e.g., Council of Europe, CAHAI (2020), The Impact of Artificial Intelligence.

Finally, **Section 8** highlights the importance of closely monitoring developments in digital technologies introduced in response to Covid-19. The crisis has made the decision-making process of governments, including adoption of new technologies and other restrictive measures, far less democratic but more secretive and non-transparent – a state of affairs that could be difficult to reverse. Countries should introduce a regulatory framework that would ensure monitoring, independent oversight mechanisms, clear requirements for transparency and impact assessment of development, deployment and use of new technologies in the public interest. These rules imposing an obligation to comply with the above-mentioned requirements would significantly reduce the possibility that countries could introduce new, highly intrusive technologies without prior assessment of their efficiency and their legal, ethical and societal impact. Likewise, such rules would prevent further use of existing technologies for completely different and unforeseen purposes. Clear regulation and control mechanisms are essential not only to protect human rights and democratic values, but also to prevent mass surveillance measures from becoming the new norm in the post-Covid-19 era. However, along with many challenges the crisis has created a unique opportunity to re-evaluate democratic governance policies and processes. It may also encourage critical assessment of the capabilities and efficiency of AI and other new technologies, and help to recognize the impact of these technologies on our rights and freedoms. Crises can also foster the development of trustworthy and human-centric AI that puts human rights, the rule of law and democracy at the forefront.

Izmantotie avoti

TIESĪBU AKTI

Starptautiskie līgumi

ANO līgumi

Apvienoto Nāciju Organizācijas Statūti. Pieņemti 26.06.1945. (Latvijā spēkā no 17.09.1991.). *Latvijas Vēstnesis*, 29.01.2018. Nr. 20.

Bērnu tiesību konvencija. Pieņemta 20.11.1989. (Latvijā spēkā no 14.05.1992.). *Latvijas Vēstnesis*, 28.11.2014., Nr. 237.

Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām. Pieņemts 16.12.1966. (Latvijā spēkā no 14.07.1992). *Latvijas Vēstnesis*, 23.04.2003., Nr. 61.

Vispārējā cilvēktiesību deklarācija. Pieņemta 10.12.1948. (Latvijā spēkā no 22.05.1990.). https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/lat.pd

Eiropas Padome

Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija. Pieņemta 04.11.1950. (EP, Latvijā spēkā no 27.06.1997.). *Latvijas Vēstnesis*, 13.06.1997., Nr. 144/145.

Konvencija par kibernoziegumiem. Pieņemta 23.11.2001. (EP, Latvijā spēkā no 01.06.2007.). *Latvijas Vēstnesis,* 26.10.2001., Nr. 171.

Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi. Pieņemta 28.01.1981. (EP, Latvijā spēkā no 01.09.2001.). *Latvijas Vēstnesis*, 12.04.2001., Nr. 59.

Protokols, ar ko groza Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu apstrādi. *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Pieņemts 10.10.2018. https://rm.coe.int/16808ac918

Eiropas Savienības tiesību akti

Eiropas Savienības Pamattiesību harta. Pieņemta 07.12.2000. OV C 2020/239, 07.06.2016.

Līgums par Eiropas Savienības darbību (konsolidētā versija). OV C 326/47. 26.10.2012.

Līgums par Eiropas Savienību, 1992. OV C 325, 24.12.2002.

Līgums par Eiropas Savienību (konsolidētā versija), OV C 115/13, 09.05.2008.

Nolīgums starp Amerikas Savienotajām Valstīm un Eiropas Savienību par pasažieru datu reģistra datu izmantošanu un pārsūtīšanu Amerikas Savienoto Valstu Iekšzemes drošības departamentam. OV L 215, 11.08.2012.

Nolīgums starp Eiropas Savienību un Amerikas Savienotajām Valstīm par tādu finanšu ziņojumapmaiņas datu apstrādi un nodošanu, kurus Eiropas Savienība dara pieejamus Amerikas Savienotajām Valstīm, lai īstenotu Teroristu finansēšanas izsekošanas programmu. OV L 8, 13.01.2010. (spēkā līdz 31.10.2010.).

Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti. *OV L* 281, 23.11.1995.

Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju). *OV L* 201, 31.07.2002.

Eiropas Parlamenta un Padomes Direktīva 2006/24/EK (2006. gada 15. marts) par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK. *OV L* 105, 13.04.2006. (spēkā līdz 03.05.2006).

Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI. *OV L* 119, 04.05.2016.

Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā. *OV L* 194, 19.07.2016.

Eiropas Parlamenta un Padomes Direktīva (ES) 2019/1024 (2019. gada 20. jūnijs) par atvērtajiem datiem un publiskā sektora informācijas atkalizmantošanu. *OV L* 172, 26.06.2019.

Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (Dokuments attiecas uz EEZ). *OV L* 119, 04.05.2016.

Eiropas Parlamenta un Padomes Regula (ES) 2016/794 (2016. gada 11. maijs) par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu) un ar kuru aizstāj un atceļ Padomes Lēmumus 2009/371/TI, 2009/934/TI, 2009/935/TI, 2009/936/TI un 2009/968/TI. *OV L* 135, 24.05.2016.

Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK. *OV L* 295/39, 21.11.2018.

Eiropas Parlamenta un Padomes Regula (ES) 2018/1727 (2018. gada 14. novembris) par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (*Eurojust*) un ar ko aizstāj un atceļ Padomes Lēmumu 2002/187/TI. *OV L* 295, 21.11.2018.

Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā. *OV L* 303/59, 28.11.2018.

Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (Dokuments attiecas uz EEZ). *OV L* 151, 07.06.2019.

Eiropas Parlamenta un Padomes Regula (ES) 2022/868 (2022. gada 30. maijs) par Eiropas datu pārvaldību un ar ko groza Regulu (ES) 2018/1724 (Datu pārvaldības akts) (Dokuments attiecas uz EEZ). *OV L* 152, 03.06.2022.

Eiropas Parlamenta un Padomes Regula (ES) 2022/1925 (2022. gada 14. septembris) par sāncensīgiem un godīgiem tirgiem digitālajā nozarē un ar ko groza Direktīvas (ES) 2019/1937 un (ES) 2020/1828 (Digitālo tirgu akts) (Dokuments attiecas uz EEZ). *OV L* 265, 12.10.2022.

Eiropas Parlamenta un Padomes Regula (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts) (Dokuments attiecas uz EEZ). *OV L* 227, 27.10.2022.

Komisijas Ieteikums (ES) 2020/518 (2020. gada 8. aprīlis) par vienotu Savienības rīkkopu tehnoloģiju un datu izmantošanai ar mērķi apkarot Covid-19 krīzi un iziet no tās, it īpaši attiecībā uz mobilajām lietotnēm un anonimizētu mobilitātes datu izmantošanu. *OV L* 114/7, 14.04.2020.

Padomes Regula (ES) 2017/1939 (2017. gada 12. oktobris), ar ko īsteno ciešāku sadarbību Eiropas Prokuratūras (EPPO) izveidei. *OV L* 283, 31.10.2017.

Latvijas tiesību akti

Latvijas Republikas Satversme. Pieņemta 15.02.1922. (spēkā no 07.11.1922.). Latvijas Vēstnesis, 01.07.1993., Nr. 43.

Elektronisko sakaru likums. Pieņemts 28.10.2004. *Latvijas Vēstnesis*, 17.11.2004., Nr. 183.

Fizisko personu datu apstrādes likums. Pieņemts 21.06.2018. *Latvijas Vēstnesis*, 04.07.2018., Nr. 132.

Informācijas sabiedrības pakalpojumu likums. Pieņemts 04.11.2004. *Latvijas Vēstnesis*, 17.11.2004., Nr. 183.

Informācijas tehnoloģiju drošības likums. Pieņemts 28.10.2010. *Latvijas Vēstnesis*, 10.11.2010., Nr. 178.

Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā. LV likums. Pieņemts 08.07.2019. *Latvijas Vēstnesis*, 22.07.2019., Nr. 147.

MK noteikumi Nr. 442. Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām. Pieņemti 28.07.2015. Latvijas Vēstnesis, 03.08.2015., Nr. 149.

Eiropas Savienības tiesību aktu projekti

Eiropas Komisija. (2017). Priekšlikums. Eiropas Parlamenta un Padomes regula par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula). https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX:52017PC0010

Eiropas Komisija. (2020). Priekšlikums. Eiropas Parlamenta un Padomes regula par saskaņotiem noteikumiem par taisnīgu piekļuvi datiem un to lietošanu (Datu akts). https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52022PC0068

Eiropas Komisija. (2021). Priekšlikums. Eiropas Parlamenta un Padomes regula, kas nosaka saskaņotas normas mākslīgā intelekta jomā (Mākslīgā intelekta akts) un groza dažus Savienības leģislatīvos aktus. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

Eiropas Komisija. (2021). Priekšlikums. Eiropas Parlamenta un Padomes regula par sadarbspējīgu vakcinācijas, testēšanas un pārslimošanas sertifikātu izdošanas, verifikācijas un akceptēšanas satvaru nolūkā atvieglot brīvu pārvietošanos Covid-19 pandēmijas laikā (digitālais zaļais sertifikāts). https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52021PC0130&from=EN

JURIDIKATŪRA

Eiropas Cilvēktiesību tiesas spriedumi

ECT 1978. gada 6. septembra spriedums lietā 5029/71 *Klass and Others v. Germany.*
ECT 1984. gada 2. augusta spriedums lietā 8691/79 *Malone v. The United Kingdom.*
ECT 1990. gada 24. aprīļa spriedums lietā 11105/84 *Huvig v. France.*
ECT 2000. gada 16. februāra spriedums lietā 27798/95 *Amann v. Switzerland*.
ECT 2006. gada 29. jūnija lēmums lietā 54934/00 *Weber and Saravia v. Germany.*
ECT 2007. gada 28. jūnija spriedums lietā *The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria.*
ECT 2007. gada 3. aprīļa spriedums lietā 62617/00 *Copland v. The United Kingdom.*
ECT 2008. gada 4. decembra spriedums lietās 30562/04 un 30566/04 *Marper v. the United Kingdom.*
ECT 2010. gada 18. maija spriedums lietā 26839/05 *Kennedy v. The United Kingdom.*
ECT 2010. gada 2. septembra spriedums lietā *Uzun v. Germany*.
ECT 2015. gada 4. decembra spriedums lietā 47143/06 *Roman Zakharov v. Russia.*
ECT 2016. gada 12. janvāra spriedums lietā 37138/14 *Szabó and Vissy v. Hungary.*
ECT 2017. gada 18. jūlija spriedums lietā 27473/06 *Mustafa Sezgin Tanrıkulu v. Turkey.*
ECT 2018. gada 13. septembra spriedums apvienotajās lietās 58170/13, 62322/14, 24960/15 *Big Brother Watch and Others v. The United Kingdom.*
ECT 2018. gada 19. jūnija spriedums lietā 35252/08 *Centrum för Rättvisa v. Sweden.*
ECT 2020. gada 13. februāra spriedums lietā 45245/15 *Gaughran v. The United Kingdom.*

Eiropas Savienības Tiesas nolēmumi

EST 1978. gada 31. janvāra spriedums lieta 94/77 *Fratelli Zerbone Snc* pret *Amministrazione delle finanze dello Stato*, ECLI:EU:C:1978:17.
EST 2009. gada 7. maija spriedums lietā C553/07 *Rijkeboer*, ECLI:EU:C:2009:293.
EST 2013. gada 17. oktobra spriedums lietā C-291/12, *M. Schwarz* pret *Stadt Bochum*, ECLI:EU:C:2013:670.
EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C293/12 *Digital Rights Ireland* un C594/12 *Seitlinger* u. c., ECLI:EU:C:2014:238.
EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems* pret *Data Protection Commissioner*, ECLI:EU:C:2015:650.
EST 2016. gada 21. februāra spriedums apvienotajās lietās C-203/15 *Tele2 Sverige AB* un C-698/15 *Watson* u. c., ECLI:EU:C:2016:970.
EST 2017. gada 26. jūlija atzinums 1/15 *Accord PNR UE-Canada*, ECLI:EU:C:2017:592.
EST 2020. gada 16. jūlija spriedums lietā C-311/18 *Data Protection Commissioner* pret *Facebook Ireland Limited* un *Maximillian Schrems*, ECLI:EU:C:2020:559.
EST 2020. gada 6. oktobra spriedums apvienotajās lietās C511/18 *La Quadrature du Net* u. c., C-512/18 *French Data Network* u. c. un C-520/18 *Ordre des barreaux francophones et germanophone* u. c., ECLI:EU:C:2020:791.
EST 2020. gada 6. oktobra spriedums lietā C-623/17 *Privacy International*, ECLI:EU:C:2020:790.

Latvijas Republikas Satversmes tiesas spriedumi un lēmumi

Satversmes tiesas 2012. gada 20. aprīļa sprieduma lietā Nr. 2011-16-01.
Satversmes tiesas 2016. gada 16. marta spriedumu lietā Nr. 2015-14-0103.
Satversmes tiesas 2019. gada 5. marta spriedums lietā Nr. 2018-08-03.

Satversmes tiesas 2019. gada 6. marta spriedums lietā Nr. 2018-11-01.
Satversmes tiesas 2020. gada 18. novembra spriedums lietā Nr. 2019-32-01.
Satversmes tiesas 2020. gada 20. novembra spriedums lietā Nr. 2019-33-01.
Satversmes tiesas 2022. gada 18. februāra lēmums lietā Nr. 2021-10-03.

STARPTAUTISKO ORGANIZĀCIJU DOKUMENTI

Apvienoto Nāciju Organizācija (ANO)

ANO Ģenerālās Asamblejas rezolūcija

UN General Assembly. (2013). Resolution 68/167. The right to privacy in the digital age. https://digitallibrary.un.org/record/764407/?ln=en

ANO ģenerālsekretāra stratēģija

UN. (2018). UN Secretary-General's Strategy on new technologies. https://www.un.org/en/newtechnologies/images/pdf/SGs-Strategy-on-New-Technologies.pdf

ANO Augstā cilvēktiesību komisāra birojs

OHCHR. (2014). The right to privacy in the digital age. https://digitallibrary.un.org/record/777869
OHCHR. (2011). Guiding Principles on Business and Human Rights. Implementing the United Nations "Protect, Respect and Remedy" Framework. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
OHCHR. (2018). The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. https://digitallibrary.un.org/record/777869#record-files-collapse-header

ANO Rasu diskriminācijas izskaušanas komiteja

UN Committee on the Elimination of Racial Discrimination. (2020). General recommendation No. 36. Preventing and Combating Racial Profiling by Law Enforcement Officials. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/349/50/PDF/G2034950.pdf?OpenElement

ANO Cilvēktiesību padome un ANO īpašais referents jautājumos par uzskatu un vārda brīvības tiesību veicināšanu un aizsardzību

UN Human Rights Council. (2019). Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. https://digitallibrary.un.org/record/3814512#record-files-collapse-header

ANO īpašais referents par tiesībām uz privātumu

UN Special Rapporteur on the right to privacy. (2017). Report of the Special Rapporteur on the right to privacy. https://digitallibrary.un.org/record/3845912
UN Special Rapporteur on the right to privacy. (2018). Report of the Special Rapporteur on the right to privacy. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/324/47/PDF/G1832447.pdf?OpenElement
UN Special Rapporteur on the right to privacy. (2019). Right to privacy. Report of the Special Rapporteur on the right to privacy. https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08;%20https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx

UN Special Rapporteur on the right to privacy. (2020). Draft for Consultations. Data Privacy Guidelines for the development and operation of Artificial Intelligence solutions. https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2020_Sept_draft_data_Privacy_guidelines.pdf

UN Special Rapporteur on the right to privacy. (2020). Report of the Special Rapporteur on the right to privacy. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/071/66/PDF/G2007166.pdf?OpenElement

Apvienoto Nāciju Izglītības, zinātnes un kultūras organizācija (UNESCO)

UNESCO, AHEG. (2020). Outcome document: first draft of the Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000373434

UNESCO. (2020). Composition of the Ad Hoc Expert Group (AHEG) for the Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000372991

UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137

Apvienoto Nāciju Starptautiskais Bērnu fonds (UNICEF)

UNICEF. (2020). Policy guidance on AI for children. https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

ANO Narkotiku un noziedzības novēršanas birojs (UNODC)

UNODC. (2009). Current practices in electronic surveillance in the investigation of serious and organized crime. https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf

ANO Starpreģionālais noziedzības un tieslietu pētniecības institūts (UNICRI) un Starptautiskā Kriminālpolicijas organizācija (INTERPOL)

UNICRI & INTERPOL. (2019). Artificial Intelligence and Robotics for Law Enforcement. https://unicri.it/artificial-intelligence-and-robotics-law-enforcement

Starptautiskā telekomunikāciju savienība (ITU)

ITU. (2015). Recommendation Y.3600. Big data – Cloud computing based requirements and capabilities. https://www.itu.int/rec/T-REC-Y.3600-201511-I/en

Ekonomiskās sadarbības un attīstības organizācija (OECD)

OECD. (1980). Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

OECD. (2013). The OECD Privacy Framework. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

OECD. (2017). OECD Digital Economy Outlook 2017. https://doi.org/10.1787/9789264276284-en

OECD. (2019). Artificial Intelligence in Society. https://www.oecd.org/publications/artificial-intelligence-in-society-eedfee77-en.htm

OECD. (2019). Recommendation of the Council on Artificial Intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

OECD. (2020). Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics. https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics/

Eiropas Padome

Council of Europe. (1981). Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/16800ca434

Council of Europe. (2017). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (T-PD). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. https://rm.coe.int/16806ebe7a

Council of Europe. (2018). Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/16808ac91a

Council of Europe. (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data – Consolidated text. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

Council of Europe. (2019). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). Guidelines of Artificial Intelligence and Data Protection. https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

Council of Europe (2019). Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes. https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4b

Council of Europe. (2019). Report on Artificial Intelligence and Data Protection: Challenges and Possible Remedies. https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6

Council of Europe. (2020). Digital Solutions to fight COVID-19. 2020 Data Protection Report. https://rm.coe.int/report-dp-2020-en/16809fe49c

Council of Europe. (2020). Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services. Joint statement by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb

Council of Europe. (2020). Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. https://rm.coe.int/covid19-joint-statement/16809e09f4

Council of Europe. (2020). Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

Council of Europe. (2020). Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis. https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40

Council of Europe. (2021). Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). Guidelines on Facial Recognition. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

Council of Europe, CAHAI. (2020). Feasibility Study. https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

Council of Europe, CAHAI. (2020). The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law. Report by Muller C. https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da

Council of Europe, CAHAI Secretariat. (2020). Towards regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law. https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a

Council of Europe Commissioner for Human Rights. (2019). Unboxing Artificial Intelligence: 10 steps to protect Human Rights. Recommendation. https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

Council of Europe. Committee of Experts on Internet Intermediaries (MSI-NET). (2018). Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

Council of Europe. Committee of Ministers. (1973). Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830

Council of Europe. Committee of Ministers. (1974). Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51

Parliamentary Assembly of the Council of Europe. (1968). Recommendation 509. Human rights and modern scientific and technological developments. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en

Parliamentary Assembly of the Council of Europe. (2015). Resolution 2045. Mass surveillance. http://assembly.coe.int/nw/xml/xref/xref-xml2html-en.asp?fileid=21692&lang=en

Parliamentary Assembly of the Council of Europe. (2017). Recommendation 2102. Technological convergence, artificial intelligence and human rights. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en

Eiropas Cilvēktiesību tiesa (ECT)

European Court of Human Rights. (2020). Guide on Article 8 of the Convention – Right to respect for private and family life. https://www.echr.coe.int/documents/guide_art_8_eng.pdf

Eiropas Savienība (ES)

Eiropas Parlaments

Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_LV.html#title2

Eiropas Parlamenta 2021. gada 25. marta normatīvā rezolūcija par priekšlikumu Eiropas Parlamenta un Padomes regulai, ar ko izveido Savienības režīmu divējāda lietojuma preču eksporta, pārvadājumu, starpniecības, tehniskās palīdzības un tranzīta kontrolei (pārstrādāta redakcija). https://www.europarl.europa.eu/doceo/document/TA-9-2021-0101_LV.html

European Parliament. (2020). Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies. https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html

European Parliament. Committee on Civil Liberties, Justice and Home Affairs (LIBE). (2020). Draft Report on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)), LIBE, Rapporteur Tudor Ciuhodaru. https://www.europarl.europa.eu/doceo/document/LIBE-PR-652625_EN.pdf

Eiropas Komisija

European Commission. (2019). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Building Trust in Human Centric Artificial Intelligence. https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence

European Commission. (2020). Inception Impact Assessment. Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Requirements-for-Artificial-Intelligence

European Commission. (2020). Joint Communication to the European Parliament, the European Council and the Council. A new EU-US agenda for global change. https://ec.europa.eu/info/sites/default/files/joint-communication-eu-us-agenda_en.pdf

European Commission. (2020). White Paper. On Artificial Intelligence – A European approach to excellence and trust. https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European Commission. Expert Group on Liability and New Technologies – New Technologies Formation. (2019). Liability for Artificial Intelligence and Other Emerging Digital Technologies. https://op.europa.eu/publication/manifestation_identifier/PUB_DS0319853ENN

Eiropas Komisija. (2015). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Digitālā vienotā tirgus stratēģija Eiropai. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex%3A52015DC0192

Eiropas Komisija. (2018). Komisijas paziņojums Eiropas Parlamentam, Eiropadomei, Padomei, Eiropas Ekonomikas un sociālajai komitejai un Reģionu komitejai. Koordinētais mākslīgā intelekta plāns. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52018DC0795&from=EN

Eiropas Komisija. (2018). Komisijas paziņojums. Mākslīgais intelekts Eiropai. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52018DC0237&from=EN

Eiropas Komisija. (2020). Baltā grāmata par mākslīgo intelektu. Eiropiska pieeja – izcilība un uzticēšanās. https://op.europa.eu/lv/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

Eiropas Komisija. (2020). Komisijas paziņojums. Norādījumi par lietotnēm, kas sniedz atbalstu cīņā pret Covid-19 pandēmiju saistībā ar datu aizsardzību. *OV C* 124/1, 17.04.2020. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020XC0417(08)&from=EN

Eiropas Komisija (2020). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Eiropas Datu stratēģija. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52020DC0066

Eiropas Komisija (2020). Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Eiropas digitālās nākotnes veidošana. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52020DC0067

Eiropas Komisija. (2020). Komisijas ziņojums Parlamentam, Padomei un Eiropas Ekonomikas un sociālo lietu komitejai. Ziņojums par mākslīgo intelektu, lietu internetu un robotiku drošuma un atbildības aspektā. https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020DC0064&from=en

Eiropas Komisija. (2020). Kopīgais Eiropas ceļvedis Covid-19 ierobežošanas pasākumu atcelšanai 2020/C 126/01. https://op.europa.eu/lv/publication-detail/-/publication/14188cd6-809f-11ea-bf12-01aa75ed71a1

Eiropas Savienības Mākslīgā intelekta augsta līmeņa ekspertu grupa (AI HLEG)

AI HLEG. (2019). A definition of artificial intelligence: main capabilities and scientific disciplines. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

AI HLEG. (2019). Ethics Guidelines for Trustworthy AI. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

AI HLEG. (2019). Policy and investment recommendations for trustworthy Artificial Intelligence. https://www.europarl.europa.eu/italy/resource/static/files/import/intelligenza_artificiale_30_aprile/ai-hleg_policy-and-investment-recommendations.pdf

AI HLEG. (2020). Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment. https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

Eiropas Datu aizsardzības kolēģija (Europen Data Protection Board, EDPB), Eiropas Datu aizsardzības uzraudzītājs (European Data Protection Supervisor, EDPS)

EDPS. (2015). Opinion 4/2015 Towards a New Digital Ethics Data, Dignity and Technology. https://edps.europa.eu/sites/default/files/publication/15-09-11_data_ethics_en.pdf

EDPS. (2018). Opinion 3/2018. EDPS Opinion on online manipulation and personal data. https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

EDPS. (2019). EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en

EDPB. (2019). Guidelines 3/2019 on processing of personal data through video devices. Version for public consultation. Adopted on 10 July 2019. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

EDPB. (2019). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

EDPB. (10 June, 2020). Response to MEPs Sophie in ‘t Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI. https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en

EDPB. (2020). Guidelines 3/2019 on processing of personal data through video devices. Version 2.0. Adopted on 29 January 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

EDPB, EDPS. (2021). EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate). https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042021-proposal_en

EDPB, EDPS. (2021). EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en

Eiropas Datu aizsardzības kolēģija. (2020). Ieteikumi 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_lv

Eiropas Datu aizsardzības kolēģija. (2020). Pamatnostādnes 04/2020 par atrašanās vietas datu un kontaktu izsekošanas rīku izmantošanu saistībā ar Covid-19 uzliesmojumu. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_lv.pdf

Eiropas Datu aizsardzības uzraudzītājs. (2018). Eiropas Datu aizsardzības uzraudzītāja atzinuma kopsavilkums par priekšlikumu regulai par Savienības pilsoņu personas apliecību un citu dokumentu drošības uzlabošanu. https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_summary_lv_0.pdf

29. panta darba grupa

Article 29 Data Protection Working Party. (2010). Opinion 3/2010 on the principle of accountability. http://www.dataprotection.ro/servlet/ViewDocument?id=654

Article 29 Data Protection Working Party. (2012). Opinion 3/2012 on developments in biometric technologies. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

Article 29 Data Protection Working Party. (2016). Guidelines on Data Protection Officers ('DPOs'). https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

Article 29 Data Protection Working Party. (2016). Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees). https://ec.europa.eu/newsroom/article29/items/640363/en

Article 29 Data Protection Working Party. (2017, as last revised and adopted 2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/612053

Article 29 Data Protection Working Party. (2017). Guidelines on Consent under Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/623051/en

Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"

for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/611236/en

Article 29 Data Protection Working Party. (2017). Guidelines on transparency under Regulation 2016/679. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Eiropas Savienības Kiberdrošības aģentūra (ENISA)

ENISA. (2015). Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. https://www.enisa.europa.eu/publications/big-data-protection

ENISA. (2016). Privacy Enhancing Technologies: Evolution and State of the Art, A Community Approach to PETs Maturity Assessment. https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art

ENISA. (2017). Handbook on Security of Personal Data Processing. https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

Eiropas Savienības Pamattiesību aģentūra

ES Pamattiesību aģentūra, ECT, EP, EDAU. (2018). Rokasgrāmata par Eiropas tiesību aktiem datu aizsardzības jomā. 2018. gada izdevums. https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

FRA. (2018). Handbook on European non-discrimination law. 2018 edition. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-non-discrimination-law-2018_en.pdf

FRA. (2018). Preventing unlawful profiling today and in the future: a guide. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

FRA. (2018). The revised Visa Information System and its fundamental rights implications. https://fra.europa.eu/en/opinion/2018/visa-system

FRA. (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement. https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

FRA. (2020). Coronavirus pandemic in the EU – Fundamental Rights Implications – Bulletin 2. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf

FRA. (2020). Getting the future right. Artificial intelligence and fundamental rights. https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

CITI JURIDISKĀS PRAKSES MATERIĀLI

Latvija

Datu valsts inspekcija. (2018). Apstrādes darbību veidi, attiecībā uz kuriem ir jāveic datu aizsardzības ietekmes novērtējums saskaņā ar VDAR 35. panta 4. punktu. https://www.dvi.gov.lv/lv/media/92/download

VARAM. (2020). Informatīvais ziņojums "Par mākslīgā intelekta risinājumu attīstību". https://www.varam.gov.lv/lv/jauns-informativais-zinojums-par-maksliga-intelekta-risinajumu-attistibu

Apvienotās Karalistes Informācijas komisāra birojs (ICO)

ICO. Data protection by design and by default. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

ICO. Data Protection Impact Assessments (DPIAs). https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/
ICO. (2023). Guidance on AI and data protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/
ICO. How should we assess security and data minimisation in AI? https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/
ICO. (2019). ICO investigation into how the police use facial recognition technology in public places. https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

Lūgums sniegt prejudiciālu nolēmumu

Lūgums sniegt prejudiciālu nolēmumu, ko 2020. gada 27. maijā iesniedza *Verwaltungsgericht Wiesbaden* (Vācija) – OC/*Bundesrepublik Deutschland*, EST lieta C-148/20, ES OV, C 279/30, 24.08.2020.

Literatūra

Barredo Arrieta, A., Díaz-Rodríguez N., Del Ser J., et al. (2020). Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI. *Information Fusion,* 58, pp. 82–115. https://doi.org/10.1016/j.inffus.2019.12.012
Bennett, C. J., Raab, C. D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. 2nd and updated ed. Cambridge, Mass: MIT Press.
Bernal, P. (2015). *Internet Privacy Rights Rights to Protect Autonomy*. Cambridge: Cambridge University Press, http://dx.doi.org/10.1017/CBO9781107337428
van Brakel, R. E. (2021). Rethinking predictive policing: Towards a holistic framework of democratic algorithmic surveillance. In: Schuilenburg, M., Peeters, R. (eds.), *Algorithmic Societies: Power, Knowledge and Technology in the Age of Algorithms*. Routledge, pp. 104–118.
Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81, pp. 77–91, http://proceedings.mlr.press/v81/buolamwini18a.html
Christoffersen, J. and Madsen, M. R. (2011). Introduction: The European Court of Human Rights between Law and Politics. In: Christoffersen, J. and Madsen, M. R. (eds.), *The European Court of Human Rights between Law and Politics*. Oxford: Oxford University Press.
Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the ACM* 31(5), 498-512.
Cohen, J. E. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Stan. L. Rev*., 52, pp. 1373–1438.
Couch, D. L., Robinson, P., and Komesaroff, P. A. (2020). COVID-19 – Extending Surveillance and the Panopticon. *Journal of Bioethical Inquiry*, 17, pp. 809–814. https://doi.org/10.1007/s11673-020-10036-5

Crawford, K., Roel, D., Theodora, D., et al. (2019). AI Now 2019 Report. AI Now Institute. https://ainowinstitute.org/publication/ai-now-2019-report-2

Davies, B., Innes, M., Dawson, A. (2018). An evaluation of South Wales Police's use of Automated Facial Recognition. Cardiff University. https://www.statewatch.org/media/documents/news/2018/nov/uk-south-wales-police-facial-recognition-cardiff-uni-eval-11-18.pdf

van Dijk, P., van Hoof G. J. H., van Rijn, A. B., Zwaak, L. (eds.). (2018). *Theory and Practice of the European Convention on Human Rights*. 5th ed. Cambridge; Antwerp; Portland: Intersentia.

Drechsler, L. (2021). Wanted: LED adequacy decisions How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context. *International Data Privacy Law*, 11(2), pp. 182-195. https://doi.org/10.1093/idpl/ipaa019

Dobber, T., Fathaigh, R. Ó., Zuiderveen Borgesius, F. J. (2019). The regulation of online political micro-targeting in Europe. *Internet Policy Review*, 8(4). https://doi.org/10.14763/2019.4.1440

Donath, J. (2020). Privacy and Public Space. In: *The Social Machine. Design for living online*. https://covid-19.mitpress.mit.edu/pub/8icuynaf

Dignum, V. (2019). *Responsible Artificial Intelligence. How to Develop and Use AI in a Responsible Way*. Springer.

Edwards, L. (ed.). (2019). *Law, Policy, and the Internet*. Oxford, UK; Portland, Orego: Hart Publishing.

Feldman Barrett, L., Adolphs, R., Marsella, S., et al. (2019). Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements. *Psychological Science in the Public Interest*, 20(1), 1–68. https://doi.org/10.1177/1529100619832930

Feldstein, S. (2019). The Global Expansion of AI surveillance. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

Ferguson, A. G. (2017). Big data Surveillance: The Convergence of Big data and Law Enfocement. In: Gray D., Henderson, S. E. (eds.), *The Cambridge Handbook on Surveillance Law*. Cambridge University Press, pp.171–197.

Fjeld, J., Achten, N., Hilligoss, H., et al. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Berkman Klein Center Research Publication No. 2020-1. https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y

Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. *Philosophy & Technology*, 29(4), pp. 307–12. https://doi.org/10.1007/s13347-016-0220-8

Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy and Technology*, 27, pp. 1–3. https://doi.org/10.1007/s13347-014-0157-8

François, C., Allaire, J. J. (2018). *Deep Learning with R*. Shelter Island, NY: Manning Publications Co.

Fussey, P., Murray, D. (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex, Human Rights Centre. https://repository.essex.ac.uk/24946/

Fussey, P., Murray, D. (2020). Policing Uses of Live Facial Recognition in the United Kingdom. In: Kak, A. (ed.), *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute, pp. 78–85. https://ainowinstitute.org/regulatingbiometrics.html

Gonzelez Fuster, G. (2020). Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf

Gstrein, O. J. (2020). Mapping Power and Jurisdiction on the Internet through the Lens of Government-Led Surveillance. *Internet Policy Review*, 9(3). https://doi.org/10.14763/2020.3.1497

Hagendorff, T. (2020). The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds & Machines,* 30, pp. 99–120. https://doi.org/10.1007/s11023-020-09517-8

Hamon, R., Junklewitz, H. and Sanchez, M. J. (2020). Robustness and Explainability of Artificial Intelligence. Publications Office of the European Union, Luxembourg. http://dx.doi.org/10.2760/57493

Harari, Y. N. (2018). *21 Lessons for the 21st Century*. New York: Spiegel & Grau.

Hawkin, S. (2018). *Brief Answers to the Big Questions*. United States: Bantam.

Jobin, A., Ienca, M., Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, pp. 389–399. https://doi.org/10.1038/s42256-019-0088-2

Kindt, E. (2020). A First Attempt at Regulating Biomentric Data in the European Union. In: Kak, A. (ed.). *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute, pp. 62–68. https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions

Kak, A. (ed.). (2020). Regulating Biometrics: Global Approaches and Urgent Questions. AI Now Institute. https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions

Kazim, E., Denny, D. M. T., Koshiyama, A. (2021). AI Auditing and Impact Assessment: According to the UK Information Commissioner's Office. *AI and Ethics*, 1, pp. 301–310. https://doi.org/10.1007/s43681-021-00039-2

Kitchin, R. (2020). Civil Liberties or Public Health, or Civil Liberties and Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19. *Space and Polity*, 24(3), pp. 362–381. https://doi.org/10.1080/13562576.2020.1770587

Kuner, C., Bygrave L. A., Docksey C. (eds.). (2019). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, United Kingdom: Oxford University Press.

Ķinis, U. (2020). Kiberdrošība – tiesiski aizsargājama vērtība. *Jurista Vārds,* 06.10.2020., Nr. 40.

Leslie, D. (2020). Understanding bias in facial recognition technologies: an explainer. The Alan Turing Institute. https://doi.org/10.5281/zenodo.4050457

Lewandowsky, S., Smillie, L., Garcia, D., et al. (2020). Technology and Democracy: Understanding the influence of online technologies on political behaviour and decision-making. Publications Office of the European Union, Luxembourg. https://data.europa.eu/doi/10.2760/709177

Līce, K., Vītola, L. E. (2020). Deklarācija starptautiskajām cilvēktiesību organizācijām par ārkārtējo situāciju Latvijā. *Jurista Vārds*, 14.04.2020., Nr. 15.

Lloyd, I. J. (2020). *Information Technology Law*. (9th ed). Oxford: Oxford University Press.

Manokha, I. (2018). Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance & Society*, 16(2), pp. 219–237. https://doi.org/10.24908/ss.v16i2.8346

Mantelero, A. (2020). Regulating AI within the Human Rights Framework: A Roadmapping Methodology. In: Czech, P., Hesch, L., Lukas, K., Nowak, M., Oberleitner, G. (eds.), *European Yearbook on Human Rights.* Interesentia, pp. 477–502.

Mantelero, A. (2018). AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment. *Computer Law & Security Review*, 34(4), pp. 754–772. https://doi.org/10.1016/j.clsr.2018.05.017

Mantelero, A. (2017). Regulating Big Data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer Law & Security Review,* 33, pp. 584–602.
Marsden, C., Meyer, T. European Parliament. Panel for the Future of Science and Technology. European Science Media-Hub. (2019). Regulating Disinformation with Artificial Intelligence: Effects of Disinformation Initiatives on Freedom of Expression and Media Pluralism. European Union. https://data.europa.eu/doi/10.2861/003689
Mayer-Schonberger V., Cukier K. (2017). *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight*. London: John Murray.
McCrudden, C. (2008). Human Dignity and Judicial Interpretation of Human Rights, *European Journal of International Law*, 19(4), pp. 655–724. https://doi.org/10.1093/ejil/chn043
McDaniel, J. L. M., Pease, K. G. (2021). Introduction. In: McDaniel, J. L. M., Pease, K. G. (eds.), *Predictive Policing and Artificial Intelligence*. Routledge, pp. 1–38.
Mcstay, A. (2020). Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy, Big Data & Society, 7(1). https://doi.org/10.1177/2053951720904386
Michalski, D., Yiu, S. Y., & Malec, C. (2018, February). The impact of age and threshold variation on facial recognition algorithm performance using images of children. In: *2018 International Conference on Biometrics (ICB),* pp. 217–224, IEEE. https://doi.org/10.1109/ICB2018.2018.00041
Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1, pp. 501–507. https://doi.org/10.1038/s42256-019-0114-4
Monahan T., Wood, D. M. Introduction. Surveillance Studies as a Transdisciplinary Endeavor. In: Monahan, T., Wood, D. M. (eds.), (2018). *Surveillance Studies: A Reader*. New York: Oxford University Press.
Monti, A., Wacks, R. (2019). *Protecting Personal Information: The Right to Privacy Reconsidered*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509924882
Moore, P. V. (2020). *Data subjects, digital surveillance, AI and the future of work*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf
Moraes, T. G., Almeida, E. C., de Pereira, J. R. L. (2021). Smile, You Are Being Identified! Risks and Measures for the Use of Facial Recognition in (Semi-)Public Spaces. *AI and Ethics,* 1, pp. 159–172. https://doi.org/10.1007/s43681-020-00014-3
Moreham, N. A. (2006). Privacy in Public Places. *Cambridge Law Journal*, 65(3), pp. 606–635. https://doi.org/10.1017/S0008197306007240
Nemitz, P. (2018). Constitutional Democracy and Technology in the Age of Artificial Intelligence. *Philos. Trans. R. Soc. A-Math. Phys. Eng. Sci.,* 376(2133). https://doi.org/10.1098/RSTA.2018.0089
Nemitz, P. (2018). Profiling the European Citizen: Why today's democracy needs to look harder at the negative potential of new technology than at its positive potential. In: Bayamlioğlu, E., Baraliuc, I., Janssens, L. u. a. (eds.), *Being Profiled: Cogitas Ergo Sum. 10 Years of Profiling the European Citizen.* Amsterdam: Amsterdam University Press, pp. 8–11. https://doi.org/10.2307/j.ctvhrd092.3
Nesterova, I. (2019). Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards. In: Ulrich, G., Ziemele, I. (eds.), *How International Law Works in Times of Crisis*. Oxford University Press, pp. 109–125.

Nijsingh, N., van Bergen, A., Wild, V. (2020). Applying a Precautionary Approach to Mobile Contact Tracing for COVID-19: The Value of Reversibility. *Journal of Bioethical Inquiry*, 17, pp. 823–827. https://doi.org/10.1007/s11673-020-10004-z

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif: Stanford Law Books.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review,* 79(119). https://core.ac.uk/download/pdf/267979739.pdf

Osipova, S. (2020). Bioethics in Correlation with the Principle of Human Dignity. *Journal of the University of Latvia. Law*, 13, pp. 121–136. https://doi.org/10.22364/jull.13.07

Pati, R. (2009). *Due Process and International Terrorism*. Leiden, Boston: Nijhoff.

Pauwels, E. (2020). Artificial Intelligence and data capture technologies in violence and conflict prevention. https://www.globalcenter.org/wp-content/uploads/2020/10/GCCS_AIData_PB_H.pdf

Perry, W. L. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND.

Rainey, B., McCormick, P., Ovey, C. (2021). *Jacobs, White, and Ovey: The European Convention on Human Rights*. Oxford University Press.

Regan, P. M. (2009). *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill, NC: The University of North Carolina Press.

Reisman, D., Schultz, J., Crawford, K., Whittaker, M. (2018). Algorithmic Impact Assessments Report: A Practical Framework for Public Agency Accountability. https://ainowinstitute.org/publication/algorithmic-impact-assessments-report-2

Rouhiainen, L. (2019). *Artificial Intelligence: 101 Things You Must Know Today about Our Future*, CreateSpace Independent Publishing Platform.

Rudgard, S. (2018). Origins and Historical Context of Data Protection Law. In: Ustaran, E., Lovells, H. (eds.), *European Data Protection. Law and Practice.* International Association of Privacy Professionals (IAPP).

Russel, S. J., Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*. Pearson Series in Artificial Intelligence. Hoboken: Pearson.

Ryan, M., Stahl, B. C. (2020). Artificial Intelligence Ethics Guidelines for Developers and Users: Clarifying Their Content and Normative Implications, *Journal of Information, Communication and Ethics in Society,* 19(1). https://doi.org/10.1108/JICES-12-2019-0138

Sartor, G., Lagioia, F. (2020) The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence. European Parliament. http://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

Schneier, B. (2016). *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World.* New York, London: W. W. Norton & Company.

Solove, D. J. (2009). *Understanding Privacy*. Cambridge, Massachusetts London, England: Harvard University Press.

Spadaro, A. (2020). COVID-19: Testing the Limits of Human Rights. *European Journal of Risk Regulation*, 11(2), pp. 317–325. https://doi.org/10.1017/err.2020.27

Stanley, J., Granick, J. S. (2020). The Limits of Location Tracking in an Epidemic. ACLU. https://www.aclu.org/wp-content/uploads/legal-documents/limits_of_location_tracking_in_an_epidemic.pdf

Susser, D., Roessler, B., Nissenbaum, H. (2019). Technology, Autonomy, and Manipulation. *Internet Policy Review,* 8(2). https://doi.org/10.14763/2019.2.1410

Taylor, L., Floridi L., van der Sloot B. (eds.). (2017). *Group Privacy: New Challenges of Data Technologies*. Cham: Springer International Publishing, https://doi.org/10.1007/978-3-319-46608-8

Taylor, L., van der Sloot, B., and Floridi, L. (2017). Conclusion: What Do We Know About Group Privacy? In: Taylor, L, Floridi, L., van der Sloot, B. (eds.), *Group Privacy*, pp. 225–37. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8_12

Thomson, J. J. (1975). The Right to Privacy. *Philosophy and Public Affairs*, 4(4), pp. 295–314.

Tokson, M. (2020). The Emerging Principles of Fourth Amendment Privacy. *The George Washington Law Review*, 88(1). https://www.gwlr.org/wp-content/uploads/2020/05/88-Geo.-Wash.-L.-Rev.-1.pdf

Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind 49*, pp. 433–460. https://www.csee.umbc.edu/courses/471/papers/turing.pdf

Tzanou, M. (2013). Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 3(2), https://doi.org/10.1093/idpl/ipt004

Tzanou, M. (2019). *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*. Oxford: Hart Publishing.

Vargo, D., Zhu, L., Benwell, B., Yan, Z. (2021). Digital Technology Use during COVID-19 Pandemic: A Rapid Review. *Human Behavior and Emerging Technologies,* 3(1), pp. 13–24. https://doi.org/10.1002/hbe2.242

Véliz, C. (2021). *Privacy Is Power: Why and How You Should Take Back Control of Your Data.* Bantam Press.

Waldron, J. (2013). Is Dignity the Foundation of Human Rights? *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.2196074

Warren, S., Brandais, L. D. (1890). The right to privacy. *Harward Law Review*, 4, pp. 193–220. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Weissman, D. (2018). Autonomy and Free Will: Autonomy and Free Will. *Metaphilosophy*, 49(5), pp. 609–645. https://doi.org/10.1111/meta.12333

Westin, A. F. (1967). *Privacy and Freedom*, New York: Atheneum.

Whitelaw, S., Mamas, A., Topol, E., van Spall, H. G. C. (2020). Applications of Digital Technology in COVID-19 Pandemic Planning and Response. *The Lancet Digital Health,* 2(8), https://doi.org/10.1016/S2589-7500(20)30142-4

Wilson, D. (2018). Algorithmic patrol: the futures of predictive policing. In: Zavrsnik, A. (ed.), *Big Data, Crime and Social Control. Routledge Frontiers of Criminal Justice*. Routledge, London.

Yeung, K., Howes, A., Pogrebna, G. (2020). AI Governance by Human Rights-Centered Design, Deliberation, and Oversight: An End to Ethics Washing. In: Dubber, M. D., Pasquale, F., and Das, S. (eds.), *The Oxford Handbook of Ethics of AI*, pp. 75–106. Oxford University Press, https://doi.org/10.1093/oxfordhb/9780190067397.013.5

Zuboff, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the new Frontier of Power.* Profile Books.

CITI MATERIĀLI (ZIŅAS, INFORMĀCIJA UN CITI INTERNETA RESURSI)

Access Now. (2018). Human rights in the age of artificial intelligence. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

Ackerman, S., Rushe, D. (3 February, 2014). The Microsoft, Facebook, Google and Yahoo release US surveillance requests. *The Guardian*. http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests

Andrews, E. L. (11 June, 2020). Governments Aren't Yet Serious About AI's Risk to Human Rights. *Stanford University Human-Centered Artificial Intelligence.* https://hai.stanford.edu/news/governments-arent-yet-serious-about-ais-risk-human-rights

Aris, B. (25 September, 2020). Belarus IT specialists develope software to identify OMON officers waring masks. *bne IntelliNews.* https://www.intellinews.com/belarus-it-specialists-develop-software-to-identify-omon-officers-wearing-masks-192747/

Article 19. (2021). Emotional Entanglement: China's emotion recognition market and its implications for human rights. https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf

Aystin, D. (16 April, 2021). Here is Your 2021 Internet Minute Infographic!: eDiscovery Trends. *eDiscoveryToday.* https://ediscoverytoday.com/2021/04/16/here-is-your-2021-internet-minute-infographic-ediscovery-trends/

Ball, S. (24 March, 2020). 100,000 cameras: Moscow uses facial recognition to enforce quarantine. *France24*. https://www.france24.com/en/20200324-100-000-cameras-moscow-uses-facial-recognition-to-enforce-quarantine

Booth, R. (3 July, 2019). Police face calls to end use of facial recognition software. *The Guardian*. https://www.theguardian.com/technology/2019/jul/03/police-face-calls-to-end-use-of-facial-recognition-software

Burgess, M. (4 September, 2019). UK police can use controversial facial recognition tech, court rules. *WIRED.* https://www.wired.co.uk/article/police-facial-recognition-south-wales-court-decision

Busvine, D. (7 April, 2020). Germany launches smartwatch app to monitor coronavirus spread. *Reuters.* https://www.reuters.com/article/us-health-coronavirus-germany-tech-idUSKBN21P1SS

Buttarelli, G. (19 October, 2018). The urgent case for a new ePrivacy law. *EDPS*. https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en

Countries are using apps and data networks to keep tabs on the pandemic. (26 March, 2020). *The Economist.* https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic

European Citizens' Initiative. Civil society initiative for a ban on biometric mass surveillance practices. https://reclaimyourface.eu

CNIL. (29 Octobre, 2019). Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position. https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

CNIL. (2019). The open source PIA software helps to carry out data protection impact assessment. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

CNIL. (9 Octobre, 2020). Reconnaissance faciale dans les aéroports: quels enjeux et quels grands principes à respecter? https://www.cnil.fr/fr/reconnaissance-faciale-dans-les-aeroports-quels-enjeux-et-quels-grands-principes-respecter

Coalition Letter Requests Federal Moratorium on the Use of Facial Recognition Technology. (16 February, 2021). *Freedom House.* https://freedomhouse.org/article/coalition-letter-requests-federal-moratorium-use-facial-recognition-technology

Council of Europe. Chart of signatures and ratifications of Treaty 108. Status as of 12/06/2021. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures

Council of Europe. Chart of signatures and ratifications of Treaty 223. Status as of 12/06/2021. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures?p_auth=iyy2ZbpX

Council of Europe. (2018). Mass surveillance. https://rm.coe.int/factsheet-on-mass-surveillance-june2018-docx/16808b3dd8

Council of Europe. Recommendations, resolutions and guidelines. https://www.coe.int/en/web/cdcj/recommendations-resolutions-guidelines

Dearden, L. (7 May, 2019). Facial recognition wrongly identifies public as potential criminals 96 % of time, figures reveal. *Independent.* https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html

DeCew, J. (2018). Privacy. In: Zalta, E. N. (ed.), *The Stanford Encyclopedia of Philosophy.* https://plato.stanford.edu/archives/spr2018/entries/privacy/

Deegan, G. (11 September, 2018). Facial imaging software detects 28 cases of welfare fraud in 2018. *The Irish Times.* https://www.irishtimes.com/news/crime-and-law/facial-imaging-software-detects-28-cases-of-welfare-fraud-in-2018-1.3626076

Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown. (16 April, 2020). *University of Oxford.* https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

Doffman, Z. (14 August, 2019). New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report. *Forbes.* https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#76f9901046c6

Dutch police facial recognition database includes 1.3 million people. (22 July, 2019). *DutchNews.nl.* https://www.dutchnews.nl/news/2019/07/dutch-police-facial-recognition-database-includes-1-3-million-people/

EDPB. (22 August, 2019). Facial recognition in school renders Sweden's first GDPR fine. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

EDPB. (21 February, 2021). Swedish DPA: Police unlawfully used facial recognition app. https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_lv

EDPS. (23 April, 2021). Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary. https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en

EDRi. EU's AI law needs major changes to prevent discrimination and mass surveillance. https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/

EDRi. (17 February, 2021). New ECI calls Europeans to stand together for a future free from harmful biometric mass surveillance. https://edri.org/our-work/new-eci-ban-biometric-mass-surveillance/

EDRi. (12 January, 2021). Re: Open letter: Civil society call for the introduction of red lines in the upcoming European Commission proposal on Artificial Intelligence. https://edri.org/wp-content/uploads/2021/01/EDRi-open-letter-AI-red-lines.pdf

E-health Network. (2020). Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States. https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19_apps_en.pdf

European Commission. (2020). Mobile applications to support contact tracing in the EU's fight against COVID-19. Progress reporting June 2020. https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf

Gallagher, R., Jona, L. (26 July, 2019). We tested Europe's new lie detector for travellers – and immediately triggered a false positive. *The Intercept.* https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/

Gellman, B., Poitras, L. (7 June, 2013). Washington Post: U.S., British intelligence mining data from nine US Internet companies in broad secret program. *Government Accountability Project.* https://whistleblower.org/in-the-news/washington-post-us-british-intelligence-mining-data-nine-us-internet-companies-broad/

Glaser, A. (12 February, 2014). Academics and Researchers Against Mass Surveillance. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2014/02/academics-and-researchers-against-mass-surveillance

Goh, B. (26 February, 2020). China rolls out fresh data collection campaign to combat coronavirus. *Reuters.* https://www.reuters.com/article/us-china-health-data-collection/china-rolls-out-fresh-data-collection-campaign-to-combat-coronavirus-idUSKCN20K0LW

Greene, J. (11 June, 2020). Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM. *The Washington Post.* https://www-washingtonpost-com.cdn.ampproject.org/c/s/www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/?outputType=amp

Google CEO backs GDPR, says privacy should not be a luxury. (22 January, 2020). *The Institute of Engineering & Technology.* https://eandt.theiet.org/content/articles/2020/01/google-ceo-backs-gdpr-says-privacy-should-not-be-a-luxury/

Government of Canada. Algorithmic Impact Assessment. https://canada-ca.github.io/aia-eia-js/

Greenwald, G., MacAskill, E. (7 June, 2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian.* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Halbfinger, D. M., Kershner, I., Bergman, R. (18 March, 2020). To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data. *The New York Times.* https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html

Harari, Y. N. (14 September, 2018). Yuval Noah Harari: the myth of freedom. *The Guardian.* https://www.theguardian.com/books/2018/sep/14/yuval-noah-harari-the-new-threat-to-liberal-democracy

Harari, Y. N. (2020). Yuval Noah Harari: "Every crisis is also an opportunity." *UNESCO Courier*, 2020-3. https://en.unesco.org/courier/2020-3/yuval-noah-harari-every-crisis-also-opportunity

Harari, Y. N. (20 March, 2020). Yuval Noah Harari: the world after coronavirus. *Financial Times.* https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Hardesty, L. (11 February, 2018). Study finds gender and skin-type bias in commercial artificial-intelligence systems. *Massachusetts Institute of Technology.* https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

Hendry, J. (19 April, 2020). WA to electronically track COVID-19 patients who defy isolation orders. *iTnews.* https://www.itnews.com.au/news/wa-to-electronically-track-covid-19-patients-who-defy-isolation-orders-546224

Hidvegi, F., Leufer, D., Massé, E. (17 February, 2021). The EU should regulate AI on the basis of rights, not risks. *Access Now*. https://www.accessnow.org/eu-regulation-ai-risk-based-approach/

Holmes, A. (12 August, 2020). Instagram could face up to $500 billion in fines in class-action lawsuit alleging it illegally harvested biometric data. *Insider.* https://www.businessinsider.com/instagram-facing-500-billion-in-fines-in-facial-recognition-lawsuit-2020-8

van den Hoven, J., Blaauw, M., Pieters, W., Warnier, M. (2014, 2019 ed.). Privacy and Information Technology. In: Zalta, E. N. (ed.), The Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/archives/sum2020/entries/it-privacy/

IEEE. (2019). Ethically Aligned Design. First Edition: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf?utm_medium=undefined&utm_source=undefined&utm_campaign=undefined&utm_content=undefined&utm_term=undefined

Ilves, I. (16 June, 2020). Why are Google and Apple dictating how European democracies fight coronavirus? *The Guardian.* https://www.theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-european-democracies-coronavirus

Ilyushina, M. (14 April, 2020). Moscow rolls out digital tracking to enforce lockdown. Critics dub it a 'cyber Gulag'. *CNN*. https://edition.cnn.com/2020/04/14/world/moscow-cyber-tracking-qr-code-intl/index.html

Jennings, R. (11 December, 2009). Google CEO: if you want privacy, do you have something to hide? *Computerworld.* https://www.computerworld.com/article/2468308/google-ceo--if-you-want-privacy--do-you-have-something-to-hide-.html

Kobie, N. (7. June, 2019) The Complicated truth about China's social credit system. *WIRED.* https://www.wired.co.uk/article/china-social-credit-system-explained

Kallingal, M. (3 April, 2020). Ankle monitors ordered for Louisville, Kentucky residents exposed to Covid-19 who refuse to stay home. *CNN*. https://edition.cnn.com/2020/04/03/us/kentucky-coronavirus-residents-ankle-monitors-trnd/index.html

Karen, H. (June 12, 2020). The two-year fight to stop Amazon from selling face recognition to the police. *MIT Technology Review.* https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/

Kayali, L. (29 October, 2019). French privacy watchdog says facial recognition trial in high schools is illegal. *POLITICO.* https://www.politico.eu/article/french-privacy-watchdog-says-facial-recognition-trial-in-high-schools-is-illegal-privacy/

Kayser-Bril, N. (18 June, 2020). At least 11 police forces use face recognition in the EU, Algorithm Watch reveals. *Algorithm Watch.* https://algorithmwatch.org/en/face-recognition-police-europe/

Kelion, L. (1 September, 2020). Coronavirus: Apple iPhones can contact-trace without Covid app. *BBC News.* https://www.bbc.com/news/technology-53987928

Kelly, E. (21 January, 2020). EU makes move to ban use of facial recognition systems. *Science|Business.* https://sciencebusiness.net/news/eu-makes-move-ban-use-facial-recognition-systems

Kharpal, A. (28 January, 2020). Big Tech's calls for more regulation offers a chance for them to increase their power. *CNBC.* https://www.cnbc.com/2020/01/28/big-techs-calls-for-ai-regulation-could-lead-to-more-power.html

Kučić, L. J. (7 July, 2020). Slovenian police acquires automated tools first, legalizes them later. *Algorithm Watch*. https://algorithmwatch.org/en/slovenia-police-face-recognition/

Kuner, C. (17 July, 2020). The Schrems II judgment of the Court of Justice and the future of data transfer regulation. *European Law Blog.* https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

Lyons, K. (13 February, 2021). Minneapolis prohibits use of facial recognition software by its police department. *The Verge*. https://www.theverge.com/2021/2/13/22281523/minneapolis-prohibits-facial-recognition-software-police-privacy

Manancourt, V. (15 June, 2020). Norway suspends contact-tracing app over privacy concerns. *POLITICO.* https://www.politico.eu/article/norway-suspends-contact-tracing-app-over-privacy-concerns/

McDonald, T. (25 September, 2020). Singapore in world first for facial verification. *BBC News.* https://www.bbc.com/news/business-54266602

Mohan, M. (12 September, 2020). More than 3,500 electronic wristband devices issued to travellers serving stay-home notices: ICA. *CNA.* https://www.channelnewsasia.com/news/singapore/electronic-wristband-devices-stay-home-notice-ica-covid-19-13105390

Moyer, E. (27 February, 2021). Facebook privacy lawsuit over facial recognition leads to $650M settlement. *Reuters.* https://www.reuters.com/article/us-facebook-privacy-lawsuit-idUSKCN25G08M

Musil, S. (14 July, 2020). Amazon, Google, Microsoft sued over photos in facial recognition database. *CNET.* https://www.cnet.com/news/amazon-google-and-microsoft-sued-over-photos-in-facial-recognition-database/

Naughton, J. (20 January, 2019). 'The goal is to automate us': welcome to the age of surveillance capitalism. *The Guardian.* https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

Nickelsburg, M. (21 January, 2020). Microsoft President Brad Smith calls for AI regulation at Davos. *GeekWire.* https://www.geekwire.com/2020/microsoft-president-brad-smith-calls-ai-regulation-davos/

O'Donoghou C., O'Brien S. (17 August, 2020). Face-off part 2: UK Court of Appeal finds deficiencies in use of automated facial recognition technology. *Technology Law Dispatch.* https://www.technologylawdispatch.com/2020/08/in-the-courts/face-off-part-2-uk-court-of-appeal-finds-deficiencies-in-use-of-automated-facial-recognition-technology

OECD. AI Policy Observatory. https://oecd.ai

Open letter to EU Member States. (11 October, 2019). *EDRi.* https://edri.org/files/eprivacy/ePrivacy_NGO_letter_20191011.pdf

Our legal action against the use of facial recognition by the french police. (21 September, 2020). La *Quadrature du Net.* https://www.laquadrature.net/en/2020/09/21/our-legal-action-against-the-use-of-facial-recognition-by-the-french-police/

Paresh, D., Jeffrey, D. (19 April, 2021). U.S. banks deploy AI to monitor customers, workers amid tech backlash. *Reuters.* https://www.reuters.com/technology/us-banks-deploy-ai-monitor-customers-workers-amid-tech-backlash-2021-04-19/

Peters, J. (9 September 2020). Portland passes strongest facial recognition ban in the US. *The Verge*. https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology

Pugh, A. (28 May, 2020). Lithuanian contact tracing app suspended. *Global Data Review.* https://globaldatareview.com/coronavirus/lithuanian-contact-tracing-app-suspended

Ravani, S. (17 July, 2019). Oakland bans use of facial recognition technology, citing bias concerns. *San Francisco Chronicle.* https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php

Rahman, M. (25 February, 2021). Here are the countries using Google and Apple's COVID-19 Contact Tracing API. *XDA Developers.* https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/

Roussi, A. (18 November, 2020). Resisting the rise of facial recognition. *Nature.* https://www.nature.com/articles/d41586-020-03188-2

Satversmes tiesa. (2020. gada 2. decembris). Satversmes tiesas priekšsēdētāja Sanita Osipova akcentē cilvēka cieņas un iecietības nozīmi pamattiesību īstenošanā. *Jurista Vārds.* https://juristavards.lv/zinas/277771-satversmes-tiesas-priekssedetaja-sanita-osipova-akcente-cilveka-cienas-un-iecietibas-nozimi-pamattiesibu-istenosana/

Serbia: Violent police crackdown against COVID-19 lockdown protesters must stop. (9 July, 2020). *Amnesty International.* https://www.amnesty.org/en/latest/news/2020/07/serbia-violent-police-crackdown-against-covid-19-lockdown-protesters-must-stop/

SHARE Foundation, Hermes Center, Bits of Freedom, ARTICLE19, Homo Digitalis and EDRi. (12 November, 2020). Campaign "Reclaim Your Face" calls for a Ban on Biometric Mass Surveillance. *EDRi.* https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/

Sherman, J. (28 January, 2020). Oh Sure, Big Tech Wants Regulation—on Its Own Terms. *WIRED*. https://www.wired.com/story/opinion-oh-sure-big-tech-wants-regulationon-its-own-terms/

Singer, N., Sang-Hun, C. (23 Mach, 2020). As Coronavirus Surveillance Escalates, Personal Privacy Plummets. *The New York Times*. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

Social Science Research Council. (2021). Surveillance and the 'New Normal' of Covid-19: Public Health, Data, and Justice. https://covid19research.ssrc.org/public-health-surveillance-and-human-rights-network/report/

Spundiņa, L. (1. oktobris, 2020). Datu valsts inspekcija neatbalsta sejas atpazīšanas video-novērošanas iekārtas. *LSM.lv.* https://www.lsm.lv/raksts/zinas/latvija/datu-valsts-inspekcija-neatbalsta-sejas-atpazisanas-videonoverosanas-iekartas.a376399/

Statement on an agreement reached between Facebook and the ICO. (30 October, 2019). *WIRED*. https://www.wired-gov.net/wg/news.nsf/articles/Statement+on+an+agreement+reached+between+Facebook+and+the+ICO+30102019151000?open

Statista. (2019). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Statt, N. (28 May 2020). ACLU sues facial recognition firm Clearview AI, calling it a 'nightmare scenario' for privacy. *The Verge.* https://www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws

Sterling, B. (17 January, 2014). Academics Against Mass Surveillance. *WIRED*. https://www.wired.com/2014/01/academics-mass-surveillance/

Stolton, S. (8 February, 2021). Commission under pressure in EU court over 'lie detector tech'. *EURACTIV.* https://www.euractiv.com/section/digital/news/aommission-under-pressure-over-lie-detector-tech-in-eu-courts/

Stolton, S. (10 November 2020). EU to restrict sale of cyber-surveillance goods to repressive regimes. *EURACTIV.* https://www.euractiv.com/section/digital/news/eu-to-restrict-sale-of-cyber-surveillance-goods-to-repressive-regimes/

Stone, M., Bartz, D. (8 January, 2021). Some U.S. Capitol rioters fired after internet detectives identify them. *Reuters.* https://www.reuters.com/article/us-usa-election-protests-fallout-idUSKBN29C36M

Swisher, K. (27 November, 2020). Amazon wants to get even closer. Skintight. *The New York Times.* https://www.nytimes.com/2020/11/27/opinion/amazon-halo-surveillance.html
Timberg, C., Harwell, D. (19 March 2020). Government efforts to track virus through phone location data complicated by privacy concerns. *The Washington Post.* https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/
The Facebook CEO Chellenges the social norm of Privacy. (12 January, 2010). *Reuters.* https://www.reuters.com/article/urnidgns852573c400693880002576a80069db04/facebook-ceo-challenges-the-social-norm-of-privacy-idUS174222527820100112
The Global Partnership on Artificial Intelligence. https://gpai.ai
Ulmer, A., Siddiqui, Z. (17 February, 2020). India's use of facial recognition tech during protests causes stir. *Reuters.* https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ
UN News. (5 November, 2018). 'Warp speed' technology must be 'force for good' UN chief tells web leaders. https://news.un.org/en/story/2018/11/1024982
UNCTAD. Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
Vinocur, N. (30 October, 2020). French politicians urge deployment of surveillance technology after series of attacks. *POLITICO*. https://www.politico.eu/article/french-politicians-urge-deployment-of-surveillance-technology-after-series-of-attacks/
Wakefield, J. (26 May, 2021). AI emotion-detection software tested on Uyghurs. *BBC News.* https://www.bbc.com/news/technology-57101248
WHO. (13 March, 2020). WHO Director-General's opening remarks at the media briefing on COVID-19 – 13 March 2020. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-mission-briefing-on-covid-19---13-march-2020
Wiewiórowski, W. (30 April, 2020). Carrying the torch in times of darkness. *EDPS.* https://edps.europa.eu/press-publications/press-news/blog/carrying-torch-times-darkness_en
Wong, Q. (27 March, 2019). Why facial recognition's racial bias problem is so hard to track. *CNET.* https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack/
Ziemele, I. (31 January, 2020). Opening of the Judicial Year Seminar. The European Convention on Human Rights: Living Instrument at 70 – Science and Technology. https://echr.coe.int/Documents/Speech_20200131_Ziemele_JY_ENG.pdf

Jēdzienu rādītājs

Irēna Barkāne
Cilvēktiesību nozīme mākslīgā intelekta laikmetā
Privātums, datu aizsardzība un regulējums
masveida novērošanas novēršanai

LU Akadēmiskais apgāds
Aspazijas bulvāris 5–132, Rīga, LV-1050, Latvija
www.apgads.lu.lv
Interneta grāmatnīca: gramatas.lu.lv

Iespiests SIA "Jelgavas tipogrāfija"