EDPB-EDPS

Atzinums 5/2021

par Ierosinājumu Eiropas Parlamenta un Padomes regulai, kurā ir izklāstīti saskaņotie noteikumi par mākslīgo inteliģenci (Mākslīgās inteliģences akts)

2021. gada 18. jūnijs

Kopsavilkums

Eiropas Komisija 2021. gada 21. aprīlī iesniedza savu Ierosinājumu par Eiropas Parlamenta un Padomes regulu, kurā ir izklāstīti saskaņotie noteikumi par mākslīgo inteliģenci (turpmāk tekstā "Ierosinājums"). Eiropas Datu aizsardzības kolēģija un Eiropas Datu aizsardzības uzraudzītājs atzinīgi vērtē likumdevēja bažas par mākslīgā intelekta (MI) izmantošanu Eiropas Savienībā (ES) un uzsver, ka Ierosinājumam ir ļoti svarīgi **datu aizsardzības implikācijām**.

EDAK un EDAU norāda, ka ierosinājuma **juridiskais pamats** pirmkārt ir Līguma par Eiropas Savienības darbību (LESD) 114. pants. Turklāt Ierosinājuma pamatā ir arī LESD 16. pants, ciktāl tas satur īpašus noteikumus par personu aizsardzību attiecībā uz personas datu apstrādi, jo īpaši ierobežojumus MI sistēmu izmantošanai "reāllaika" attālinātai biometriskai identifikācijai publiski pieejamās vietās tiesībaizsardzības nolūkos. EDAK un EDAU atgādina, ka saskaņā ar Eiropas Savienības Tiesu (EST) LESD 16. pants nodrošina piemērotu juridisko pamatu gadījumos, kad personas datu aizsardzība ir viens no ES likumdevēja pieņemto noteikumu galvenajiem mērķiem vai sastāvdaļām. LESD 16. panta piemērošana ietver arī **nepieciešamību nodrošināt neatkarīgu uzraudzību** attiecībā uz personas datu apstrādes prasību ievērošanu, kā noteikts arī ES Pamattiesību hartas 8. pantā.

Attiecībā uz **Ierosinājuma darbības jomu** EDAK un EDAU ļoti atzinīgi vērtē to, ka tas attiecas arī uz MI sistēmu nodrošināšanu un izmantošanu, ko veic ES iestādes, struktūras vai aģentūras. Tomēr **starptautiskās tiesībaizsardzības sadarbības izslēgšana no Ierosinājuma darbības jomas** rada nopietnas bažas EDAK un EDAU, jo šāda izslēgšana rada ievērojamu apiešanas risku (piemēram, trešās valstis vai starptautiskās organizācijas, kas izmanto augsta riska pielietojumos, uz kuriem atsaucas ES valsts iestādes).

EDAK un EDAU **atzinīgi vērtē uz risku balstīto pieeju**, kas ir Ierosinājuma pamatā. Tomēr šī pieeja būtu jāprecizē un jēdziens "pamattiesību risks" būtu jāsaskaņo ar VDAR un Regulu (ES) 2018/1725 (EUDPR), jo tiek ņemti vērā personas datu aizsardzību saistītie aspekti.

EDAK un EDAU piekrīt Ierosinājumam, norādot, ka **MI kā augsta riska sistēmas klasificēšana ne vienmēr nozīmē, ka tā ir likumīga** pati par sevi un lietotājs to var izmantot kā tādu. Pārzinim **var būt jāievēro papildu prasības, kas izriet no ES datu aizsardzības tiesību aktiem**. Turklāt atbilstībai juridiskajām saistībām, kas izriet no Savienības tiesību aktiem (tostarp personas datu aizsardzības jomā), vajadzētu būt priekšnosacījumam, kas ļauj iekļūt Eiropas tirgū kā ar CE zīmi marķētam produktam. Šajā nolūkā EDAK un EDAU uzskata, ka **prasība nodrošināt VDAR un EUDPR ievērošanu būtu jāiekļauj III sadaļas 2. nodaļā**. Turklāt EDAK un EDAU uzskata par nepieciešamu pielāgot Ierosinājuma atbilstības novērtēšanas procedūru tā, lai trešās puses vienmēr veiktu augsta riska MI sistēmu *ex-ante* atbilstības novērtējumus.

Ņemot vērā lielo diskriminācijas risku, Ierosinājumā tiek aizliegta "sociālā vērtēšana", ja to veic "noteiktā laikposmā" vai arī "valsts iestādes vai to vārdā". Tomēr arī privāti uzņēmumi, piemēram, sociālie tīkli un mākoņpakalpojumu sniedzēji, var apstrādāt lielu personas datu apjomu un veikt sociālo vērtēšanu. Līdz ar to **jaunajā MI regulā būtu jāaizliedz jebkāda veida sociālie vērtējumi**.

Attālināta personu biometriskā identifikācija publiski pieejamās vietās rada augstu risku saistībā ar ielaušanos personu privātajā dzīvē, un tas nopietni ietekmē iedzīvotāju vēlmi būt anonīmiem sabiedriskās vietās. Šo iemeslu dēļ EDAK un EDAU **aicina noteikt vispārēju aizliegumu MI izmantošanai, lai automatizēti atpazītu cilvēka iezīmes publiski pieejamās vietās** — piemēram, sejas, bet arī gaitu, pirkstu nospiedumus, DNS, balsi, taustiņsitienus un citus biometriskus vai uzvedības signālus, turklāt jebkurā kontekstā. Tāpat ir ieteicams **aizliegt MI sistēmas, kurās personas pēc biometrijas tiek iedalītas kopās** atbilstoši etniskajai piederībai, dzimumam, kā arī politiskajai vai seksuālajai orientācijai vai citiem diskriminācijas iemesliem saskaņā ar Hartas 21. pantu. Turklāt EDAK un EDAU uzskata, ka MI izmantošana **fiziskas personas emociju nozīmes secināšanai ir ļoti nevēlama un būtu jāaizliedz.**

EDAK un EDAU atzinīgi vērtē **EDAU izraudzīšanu par kompetento iestādi un tirgus uzraudzības iestādi Savienības iestāžu, aģentūru un struktūru uzraudzībai**. Tomēr būtu jāprecizē EDAU loma un uzdevumi, jo īpaši attiecībā uz tās kā tirgus uzraudzības iestādes lomu. Turklāt jaunajā MI regulā ir skaidri jānosaka **uzraudzības iestāžu neatkarība**, veicot uzraudzības un izpildes uzdevumus.

Datu aizsardzības iestāžu (DAI) izraudzīšana par valsts uzraudzības iestādēm nodrošinātu vairāk saskaņotu regulatīvo pieeju, palīdzētu konsekventi interpretēt datu apstrādes nosacījumus un novērstu pretrunas to izpildē starp dalībvalstīm. Līdz ar to EDAK un EDAU uzskata, ka **datu aizsardzības iestādes būtu jāieceļ par valsts uzraudzības iestādēm saskaņā ar Ierosinājuma 59. pantu.**

Ierosinājums piešķir galveno lomu Komisijai "Eiropas mākslīgā intelekta padomē" (EMIP). Šāda loma ir pretrunā ar MI Eiropas struktūras nepieciešamību būt neatkarīgai no jebkādas politiskas ietekmes. Lai nodrošinātu tās neatkarību, jaunajai MI regulai vajadzētu piešķirt **EMIP lielāku autonomiju** un nodrošināt, ka tā var rīkoties pēc savas iniciatīvas.

Ņemot vērā MI sistēmu izplatību vienotajā tirgū un pārrobežu gadījumu iespējamību, ir ārkārtīgi nepieciešama saskaņota izpilde un pienācīga kompetences sadale starp valstu uzraudzības iestādēm. EDAK un EDAU ierosina izskatīt **mehānismu, kas garantētu vienotu kontaktpunktu katrai MI sistēmai gan fiziskām personām, uz kuriem attiecas tiesību akti, gan arī uzņēmumiem.**

Attiecībā uz **smilškastēm** EDAK un EDAU **iesaka precizēt to darbības jomu un mērķus**. Turklāt ierosinājumā ir skaidri jānorāda, ka šādu smilškastu juridiskajam pamatam ir jāatbilst esošajā datu aizsardzības sistēmā noteiktajām prasībām.

Ierosinājumā izklāstītajai **sertifikācijas sistēmai trūkst skaidras saistības ar ES datu aizsardzības tiesību aktiem**, kā arī ar citiem ES un dalībvalstu tiesību aktiem, kas ir piemērojami katrai augsta riska MI sistēmas "jomai", un kuros **datu minimizēšanas un datu aizsardzības principi** netiek ņemti vērā kā viens no aspektiem, kas ir jāizskata **pirms CE zīmes iegūšanas**. Tāpēc EDAK un EDAU iesaka grozīt Ierosinājumu, lai precizētu saistību starp sertifikātiem, kas tika izdoti saskaņā ar minēto Regulu, un datu aizsardzības sertifikātiem, plombām un zīmēm. Visbeidzot DAI būtu jāiesaistās saskaņotu standartu un vispārēju specifikāciju sagatavošanā un izveidē.

Attiecībā uz **rīcības kodeksiem** EDAK un EDAU uzskata par **nepieciešamu precizēt**, vai personas datu aizsardzība ir uzskatāma par "papildu prasībām", kuras var risināt ar šiem rīcības kodeksiem, un nodrošināt, ka "tehniskās specifikācijas un risinājumi" nav pretrunā ar esošā ES datu aizsardzības regulējuma noteikumiem un principiem.

SATURA RĀDĪTĀJS

1 IEVADS 5
2 IEROSINĀJUMA GALVENO PRINCIPU ANALĪZE 7
2.1 Ierosinājuma piemērojamība un saistība ar esošo tiesisko regulējumu 7
2.2 Riska izvērtēšanā balstīta pieeja 8
2.3 Aizliegtie MI izmantošanas veidi 10
2.4 Augsta riska MI sistēmas 12
2.4.1 Ārēju trešo pušu *ex-ante* atbilstības novērtēšanas nepieciešamība 12
2.4.2 Regulas darbības jomai ir jāaptver arī jau izmantotās MI sistēmas 12
2.5 Pārvalde un Eiropas MI padome 13
2.5.1 Pārvaldība 13
2.5.2 Eiropas MI padome 15
3 MIJIEDARBĪBA AR datu aizsardzības struktūru 16
3.1 Ierosinājuma saistība ar spēkā esošajiem ES datu aizsardzības tiesību aktiem 16
3.2 Smilškaste un turpmāka apstrāde (Ierosinājuma 53. un 54. pants) 16
3.3 Pārredzamība 18
3.4 Īpašu kategoriju datu un datu, kas saistīti ar noziedzīgiem nodarījumiem, apstrāde 19
3.5 Atbilstības mehānismi 19
3.5.1 Sertifikācija 19
3.5.2 Rīcības kodeksi 20
4 SECINĀJUMS 21

Eiropas Datu aizsardzības kolēģija un Eiropas Datu aizsardzības uzraudzītājs,

ņemot vērā 42. panta 2. punktu 2018. gada 23. oktobra Regulā 2018/1725 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK,[1],

ņemot vērā EEZ līgumu un jo īpaši tā XI pielikumu un 37. protokolu, kas grozīts ar EEZ apvienotās komitejas 2018. gada 6. jūlija Lēmumu Nr. 154/2018[2];

Ņemot vērā Eiropas Datu aizsardzības uzraudzītāja un Eiropas Datu aizsardzības kolēģijas 2021. gada 22. aprīļa pieprasījumu sniegt kopīgu atzinumu par ierosinājumu regulai, kas nosaka saskaņotus noteikumus par mākslīgo intelektu (Mākslīgā intelekta likums),

IR PIEŅĒMUŠI ŠĀDU KOPĒJU ATZINUMU

1 IEVADS

1. Mākslīgā intelekta ("MI") sistēmu ieviešana ir ļoti svarīgs solis tehnoloģiju attīstībā un cilvēku mijiedarbībā ar tām. Mākslīgais intelekts ir galveno tehnoloģiju kopums, kas būtiski mainīs mūsu ikdienas dzīvi no sabiedrības un ekonomiskā viedokļa. Turpmākajos gados tiek gaidīti izšķiroši lēmumi attiecībā uz mākslīgo intelektu, jo tas mums palīdz pārvarēt dažas no lielākajām problēmām, ar kurām pašlaik saskaramies daudzās jomās, sākot no veselības aprūpes līdz mobilitātei vai no valsts pārvaldes līdz izglītībai.

2. Tomēr šie solītie uzlabojumi nav bez riska. Riski tiešām ir ļoti būtiski, ņemot vērā to, ka MI sistēmu individuālā un sociālā ietekme lielā mērā nav pieredzēta. Satura ģenerēšana, prognozēšana un lēmumu pieņemšana automatizēti, kā to dara mākslīgā intelekta sistēmas, izmantojot mašīnmācīšanās paņēmienus vai loģiku un varbūtības secināšanas noteikumus, nav tāda pati kā cilvēkiem, kuri veic šīs darbības, izmantojot radošu vai teorētisku argumentāciju un uzņemoties pilnu atbildību par sekām.

3. Mākslīgais intelekts paplašinās iespējamo prognožu apjomu daudzās jomās, sākot ar izmērāmām datu korelācijām, kas nav pamanāmas cilvēkiem, bet ir redzamas mašīnām, atvieglojot mūsu dzīvi un atrisinot daudzas problēmas, bet vienlaikus vājinās mūsu spēju cēloniski interpretēt iznākumus tā, ka tiks nopietni pārbaudīti tādi jēdzieni kā pārredzamība, cilvēka kontrole, pārskatatbildība un atbildība par rezultātiem.

4. MI dati (gan personu, gan arī citi) daudzos gadījumos ir galvenais priekšnoteikums autonomu lēmumu pieņemšanai, un tas neizbēgami ietekmēs fizisku personu dzīvi dažādos līmeņos. Tāpēc EDAK un EDAU jau šajā posmā stingri apgalvo, ka Ierosinājumam par Regulu, kurā

[1] OV L 295, 21.11.2018., 39.-98. lpp.
[2] Šajā dokumentā atsauces uz "dalībvalstīm" būtu jāsaprot kā atsauces uz "EEZ dalībvalstīm".

tiek izklāstīti saskaņoti noteikumi par mākslīgo intelektu (Mākslīgā intelekta likums) ("Ierosinājums")[3], ir **būtiska ietekme uz datu aizsardzību**.

5. Izlemšanas uzdevuma piešķiršana mašīnām, pamatojoties uz datiem, radīs fizisku personu tiesību un brīvību risku, ietekmēs viņu privāto dzīvi un var kaitēt grupām vai pat sabiedrībai kopumā. EDAK un EDAU uzsver, ka tiesības uz privāto dzīvi un personas datu aizsardzību, kas ir pretrunā pieņēmumam par mašīnu izlemšanas autonomiju, kurš ir MI koncepcijas pamatā, ir ES vērtību pīlārs, kā atzīts Vispārējā cilvēktiesību deklarācijā (12. pants), Eiropas Cilvēktiesību konvencijā (8. pants) un ES Pamattiesību hartā (turpmāk "Harta") (7. un 8. pants). Ļoti ambiciozs, tomēr nepieciešams mērķis ir saskaņot MI pielietojuma piedāvāto izaugsmes perspektīvu ar cilvēka centrālo un primāro vietu un pārākumu attiecībā pret mašīnām.

6. EDAK un EDAU atzinīgi vērtē visu MI vērtību ķēdē ieinteresēto personu iesaistīšanos regulēšanā un īpašu prasību ieviešanu risinājumu sniedzējiem, jo tām ir nozīmīga loma produktos, kuros tiek izmantotas viņu sistēmas. Tomēr ir skaidri jāapraksta un jāpiešķir dažādu pušu — MI sistēmas lietotāja, nodrošinātāja, importētāja un izplatītāja — pienākumi. Jo īpaši, apstrādājot personas datus, īpaša uzmanība ir jāpievērš šo lomu un pienākumu saskaņai ar datu pārziņa un datu apstrādātāja jēdzieniem, kas ir ietverti datu aizsardzības sistēmā, jo abas normas nav saskaņotas.

7. Ierosinājums ieņem nozīmīgu vietu cilvēka uzraudzības jēdzienā (14. pants), ko atzinīgi vērtē EDAK un EDAU. Tomēr, kā minēts iepriekš, dažu MI sistēmu spēcīgās potenciālās ietekmes uz indivīdiem vai personu grupām dēļ reālai cilvēku centralitātei ir jāizmanto augsti kvalificēta cilvēku uzraudzība un likumīga apstrāde, ciktāl šādas sistēmas balstās uz personas datu apstrādi vai apstrādā personas datus savu uzdevumu izpildes nolūkos, lai nodrošinātu tādu tiesības ievērošanu, kas nozīmē netikt pakļautam lēmumam, kura pamatā ir tikai automatizēta apstrāde.

8. Turklāt, tā kā daudziem MI pielietojumiem ir liels datu apjoms, tad Ierosinājumam ir jāveicina iecerēta un pēc noklusējuma izveidota pieeja datu aizsardzībai visos līmeņos, veicinot datu aizsardzības principu (kā paredzēts VDAR 25. pantā un EUDPR 27. pantā) efektīvu īstenošanu, izmantojot vismodernākās tehnoloģijas.

9. Visbeidzot EDAK un EDAU uzsver, ka šis kopīgais atzinums tiek sniegts tikai kā Ierosinājuma sākotnēja analīze, neskarot nekādu turpmāku novērtējumu un atzinumu par Ierosinājuma ietekmi un tā saderību ar ES datu aizsardzības tiesību aktiem.

[3] COM(2021) 206 galīgā redakcija.

2 IEROSINĀJUMA GALVENO PRINCIPU ANALĪZE

2.1 Ierosinājuma piemērojamība un saistība ar esošo tiesisko regulējumu

10. Saskaņā ar paskaidrojuma rakstu ierosinājuma **juridiskais pamats**, pirmkārt, ir LESD 114. pants, kas paredz pieņemt pasākumus iekšējā tirgus izveides un darbības nodrošināšanai[4]. Turklāt Ierosinājuma pamatā ir LESD 16. pants, *ciktāl tas satur īpašus noteikumus par fizisku personu aizsardzību attiecībā uz personas datu apstrādi*, jo īpaši ierobežojumus MI sistēmu izmantošanai "reāllaika" attālinātai biometriskai identifikācijai publiski pieejamās vietās tiesībaizsardzības nolūkos[5].

11. EDAK un EDAU atgādina, ka saskaņā ar EST LESD 16. pants nodrošina piemērotu juridisko pamatu gadījumos, kad personas datu aizsardzība ir viens no ES likumdevēja pieņemto noteikumu galvenajiem mērķiem vai sastāvdaļām[6]. LESD 16. panta piemērošana ietver arī nepieciešamību nodrošināt neatkarīgu uzraudzību attiecībā uz personas datu apstrādes prasību ievērošanu, kā noteikts arī Hartas 8. pantā.

12. EDAU un EDAK atgādina, ka vispusīga datu aizsardzības sistēma, kas ir pieņemta, pamatojoties uz LESD 16. pantu, jau pastāv, un tajā ietilpst Vispārīgā datu aizsardzības regula (VDAR)[7], Eiropas Savienības iestāžu, biroju, struktūru un aģentūru datu aizsardzības regula (EUDPR)[8] un Tiesībaizsardzības direktīva (LED)[9]. Saskaņā ar Ierosinājumu tikai papildu ierobežojumus attiecībā uz Ierosinājumā ietverto biometrisko datu apstrādi var uzskatīt par tādiem, kuru pamatā ir LESD 16. pants, un tāpēc tiem ir tāds pats juridiskais pamats kā VDAR, EUDPR vai LED. Tas būtiski ietekmē Ierosinājuma saistību ar VDAR, EUDPR un LED kopumā, kā izklāstīts turpmāk.

13. Attiecībā uz **Ierosinājuma darbības jomu** EDAK un EDAU ļoti atzinīgi vērtē to, ka Ierosinājums attiecas arī uz MI sistēmu izmantošanu, ko veic ES iestādes, struktūras vai aģentūras. Ņemot vērā to, ka MI sistēmu izmantošana šajās struktūrās var būtiski ietekmēt indivīdu pamattiesības līdzīgi izmantošanai ES dalībvalstīs, jaunajai MI regulācijas sistēmai ir obligāti jāattiecas gan uz ES dalībvalstīm, gan arī uz ES iestādēm, birojiem, struktūrām un aģentūrām, lai nodrošinātu saskaņotu pieeju visā Savienībā. Tā kā ES iestādes, biroji, struktūras un aģentūras var darboties gan kā MI sistēmu nodrošinātāji, gan arī kā lietotāji, EDAU un

[4] Paskaidrojuma raksts, 5. lpp.
[5] Paskaidrojuma raksts, 6. lpp. Skatīt arī ierosinājuma apsvērumu (2).
[6] 2017. gada 26. jūlija atzinums *PNR Canada*, atzinuma procedūra 1/15, ECLI:ES:C:2017:592, 96. punkts.
[7] 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, ar ko tiek atcelta Direktīva 95/46/EK (Vispārīgā datu aizsardzības regula) OJ L 119, 4.5.2016., 1.–88. lpp.
[8] 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, ar ko tiek atcelta Regula (EK) Nr. 45/2001 un Lēmums Nr. 1247/2002/EK, OJ L 295, 21.11.2018., 39.–98. lpp.
[9] 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/JHA, OJ L 119, 4.5.2016., 89.–131. lpp.

EDAK uzskata, ka ir pilnīgi lietderīgi šīs struktūras iekļaut Ierosinājuma darbības jomā, pamatojoties uz LESD 114. pantu.

14. Tomēr EDAK un EDAU ir nopietnas bažas par starptautiskās tiesībaizsardzības sadarbības izslēgšanu no Ierosinājuma 2. panta 4. punkta noteiktās darbības jomas. Šī izslēgšana rada ievērojamu apiešanas risku (piemēram, trešās valstis vai starptautiskas organizācijas ar augsta riska pielietojumiem, uz ko balstās ES valstu iestādes).

15. MI sistēmu izstrāde un izmantošana daudzos gadījumos ietvers personas datu apstrādi. Ārkārtīgi svarīgi ir nodrošināt skaidrību šī Ierosinājuma saistībai ar spēkā esošajiem ES tiesību aktiem par datu aizsardzību. Ierosinājums neskar un papildina GDAK, EUDPR un LED. Lai gan Ierosinājuma apsvērumos ir paskaidrots, ka MI sistēmu izmantošanai joprojām ir jāatbilst datu aizsardzības tiesību aktiem, **EDAK un EDAU stingri iesaka Ierosinājuma 1. pantā precizēt, ka Savienības tiesību akti personas datu aizsardzībai,** jo īpaši VDAR, EUDPR, e-privātuma direktīva[10] un LED, tiks piemēroti jebkurai personas datu apstrādei, kas ietilpst Ierosinājuma darbības jomā. Tāpat līdzīgā apsvērumā būtu jāprecizē, ka Ierosinājums nemēģinās ietekmēt to esošo Eiropas Savienības tiesību aktu piemērošanu, ar kuriem tiek reglamentēta personas datu apstrāde, tostarp to neatkarīgo uzraudzības iestāžu uzdevumus un pilnvaras, kuras ir kompetentas uzraudzīt atbilstību šiem instrumentiem.

2.2 Riska izvērtēšanā balstīta pieeja

16. EDAK un EDAU **atzinīgi vērtē uz risku balstīto pieeju**, kas ir Ierosinājuma pamatā. Ierosinājums attiektos uz visām MI sistēmām, tostarp tām, kas nav saistītas ar personas datu apstrādi, bet tomēr var ietekmēt intereses vai pamattiesības un brīvības.

17. EDAK un EDAU atzīmē, ka daži Ierosinājuma noteikumi neietver riskus indivīdu grupām vai sabiedrībai kopumā (piemēram, kolektīva ietekmi ar īpašu nozīmi, piemēram, grupu diskrimināciju vai politisko uzskatu paušanu sabiedriskās vietās). EDAK un EDAU iesaka vienlīdz novērtēt un mazināt sabiedriskos/grupas riskus, ko rada MI sistēmas.

18. EDAK un EDAU uzskata, ka būtu jāprecizē uz Ierosinājumu balstītā riska pieeja un jēdziens "pamattiesību risks" būtu **jāsaskaņo ar VDAR**, ciktāl tiek ņemti vērā aspekti, kas ir saistīti ar personas datu aizsardzību. Neatkarīgi no tā, vai MI sistēma attiecas uz galalietotājiem, vienkārši datu subjektiem vai citām personām, ja tekstā nav atsauces uz fizisku personu, kuru ietekmē MI sistēma, tas Ierosinājumā parādās kā akla vieta. Patiešām pienākumiem, kas tiek piemēroti darbiniekiem attiecībā uz ietekmētajām personām, vajadzētu konkrētāk izrietēt no indivīda un viņa tiesību aizsardzības. Tādējādi EDAK un EDAU mudina likumdevējus Ierosinājumā skaidri pievērsties **tiesībām un aizsardzības līdzekļiem, kas ir pieejami personām**, kuras ir pakļautas MI sistēmām.

19. EDAK un EDAU ņem vērā izvēli nodrošināt izsmeļošu **augsta riska MI sistēmu** sarakstu. Šī izvēle var radīt melnbaltu efektu ar vāju piesaistes spēju ļoti riskantās situācijās, apdraudot Ierosinājuma pamatā esošo vispārējo pieeju uz riska bāzes. Turklāt šajā augsta riska MI sistēmu

[10] 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), kas grozīta ar Direktīvu 2006/24/EK un Direktīvu 2009/136/EK.

sarakstā, kas ir sīki izklāstīts Ierosinājuma II un III pielikumā, trūkst dažu lietošanas gadījumu veidu, kas ir saistīti ar būtiskiem riskiem, piemēram, MI izmantošanas apdrošināšanas prēmijas noteikšanai vai ārstniecības vai veselības novērtēšanai veselības izpētes nolūkos. EDAK un EDAU arī uzsver, ka šie pielikumi būs regulāri jāatjaunina, lai nodrošinātu to darbības jomas atbilstību.

20. Ierosinājumā ir noteikts, ka MI sistēmas **nodrošinātājiem** ir jāveic riska novērtējums, tomēr vairumā gadījumu (datu) pārziņi būs MI sistēmu **lietotāji**, nevis nodrošinātāji (piemēram, sejas atpazīšanas sistēmas lietotājs ir "pārzinis", un tāpēc viņam nav saistošas augsta riska MI pakalpojumu sniedzēju prasības saskaņā ar Ierosinājumu).

21. Turklāt **pakalpojumu sniedzējam ne vienmēr būs iespējams novērtēt visus MI sistēmas lietojumus**. Tādējādi sākotnējais riska novērtējums būs vispārīgāks nekā tas, ko veic MI sistēmas lietotājs. Pat ja sākotnējais riska novērtējums, ko veicis pakalpojumu sniedzējs, neliecina, ka MI sistēma saskaņā ar Ierosinājumu ir "augsta riska" sistēma, tam nevajadzētu izslēgt **turpmāku (detalizētāku) novērtējumu** (ietekmes uz datu aizsardzību novērtējumu ("DPIA") saskaņā ar VDAR 35. pantu, EUDPR 39. pantu vai LED 27. pantu), **kas ir jāveic sistēmas lietotājam**, ņemot vērā lietošanas kontekstu un īpašos lietošanas gadījumus. Neatkarīgi no Ierosinājuma ir jāinterpretē, vai kāda veida apstrāde, iespējams, rada augstu risku saskaņā ar VDAR, EUDPR un LED. Tomēr MI kā "augsta riska" sistēmas klasificēšana (jo tā ietekmē pamattiesības)[11] **rada pamatu "augsta riska" pieņēmumam saskaņā ar VDAR, EUDPR un LED, ciktāl tiek apstrādāti personas dati.**

22. **EDAK un EDAU piekrīt Ierosinājumam, norādot, ka MI sistēmas klasificēšana par augsta riska sistēmu ne vienmēr nozīmē, ka tā *pati par sevi* ir likumīga un lietotājs to var izmantot kā tādu. Pārzinim var būt jāievēro papildu prasības, kas izriet no ES datu aizsardzības tiesību aktiem.** Turklāt Ierosinājuma 5. panta pamatā esošais pamatojums, ka, atšķirībā no aizliegtajām sistēmām, augsta riska sistēmas var būt principā pieļaujamas, ir jārisina un jāizkliedē Ierosinājumā, jo īpaši tāpēc, ka ierosinātā CE zīme nenozīmē, ka ar to saistītā personas datu apstrāde ir likumīga.

23. Tomēr atbilstībai juridiskajām saistībām, kas izriet no Savienības tiesību aktiem (tostarp personas datu aizsardzības jomā), vajadzētu būt priekšnosacījumam, kas ļauj iekļūt Eiropas tirgū kā ar CE zīmi marķētam produktam. Šim nolūkam EDAK un EDAU **Ierosinājuma III sadaļas 2. nodaļā iesaka iekļaut prasību par atbilstības VDAR un EUDPR nodrošināšanu**. Šīs prasības pirms CE marķējuma ir jārevidē (trešās puses revīzijā) saskaņā ar pārskatatbildības principu. Šī trešās puses novērtējuma kontekstā sākotnējais ietekmes novērtējums, kas jāveic pakalpojumu sniedzējam, būs īpaši svarīgs.

24. Ņemot vērā sarežģītību, ko izraisa MI sistēmu attīstība, ir jānorāda, ka MI sistēmu tehniskie raksturlielumi (piemēram, MI pieejas veids) varētu radīt lielākus riskus. Tāpēc, veicot MI

[11] Eiropas Savienības Pamattiesību aģentūra (FRA) jau ir pievērsusies nepieciešamībai novērtēt ietekmi uz pamattiesībām, izmantojot MI vai ar to saistītas tehnoloģijas. Savā 2020. gada ziņojumā "Pareizas nākotnes veidošana — mākslīgais intelekts un pamattiesības" FRA konstatēja "nepilnības MI izmantošanā, piemēram, prognožu politikā, medicīnas diagnozēs, sociālajos pakalpojumos un mērķtiecīgā reklāmā" un uzsvēra, ka "privātajām un sabiedriskajām organizācijām ir jāizvērtē, kā MI varētu kaitēt pamattiesībām", lai mazinātu negatīvo ietekmi uz fiziskām personām.

sistēmas riska novērtējumu, ir jāņem vērā **tehniskie raksturlielumi**, **kā arī tās īpašie lietošanas gadījumi un konteksts**, kādā sistēma darbojas.

25. Ņemot vērā iepriekš minēto, EDAKPB un EDAU Ierosinājumā iesaka precizēt, ka **pakalpojumu sniedzējam** ir jāveic sākotnējais riska novērtējums attiecīgajai MI sistēmai, **ņemot vērā lietošanas gadījumus** (jāprecizē Ierosinājumā, papildinot, piemēram, III pielikuma 1. panta a) punktu, ja MI biometrisko sistēmu lietošanas gadījumi nav minēti), un ka MI sistēmas **lietotājs** kā datu pārzinis saskaņā ar ES datu aizsardzības tiesību aktiem (ja nepieciešams) veic DPIA saskaņā ar VDAR 35. pantu, EUDPR 39. pantu un LED 27. pantu, ņemot vērā ne tikai tehnisko raksturojumu un **lietošanas gadījumu**, bet **arī īpašo kontekstu**, kurā MI darbosies.

26. Turklāt daži no Ierosinājuma III pielikumā minētajiem terminiem būtu jāprecizē — piemēram, termins "būtiski privātie pakalpojumi" vai maza apjoma pakalpojumu sniedzējs, kas izmanto kredītspējas novērtējuma MI savām vajadzībām.

2.3 Aizliegtie MI izmantošanas veidi

27. EDAK un EDAU uzskata, ka **uzmācīgi MI veidi**, jo īpaši tie, kas var ietekmēt cilvēka cieņu, ir uzskatāmi par aizliegtām MI sistēmām saskaņā ar Ierosinājuma 5. pantu, nevis vienkārši tiek klasificēti kā "augsta riska" sistēmas Ierosinājuma III pielikumā, piemēram, pie Nr. 6. Tas jo īpaši attiecas uz datu salīdzinājumiem, kas lielā mērā ietekmē arī personas, kuras nav devušas iemeslu vai ir devušas tikai nelielu iemeslu policijas novērošanai vai apstrādei, kas pārkāpj datu aizsardzības tiesību aktos noteikto mērķa ierobežojuma principu. MI izmantošanai policijas un tiesībaizsardzības jomā ir nepieciešami konkrētai jomai specifiski, precīzi, paredzami un samērīgi noteikumi, kuros ir jāņem vērā ieinteresēto personu intereses un ietekme uz demokrātiskas sabiedrības darbību.

28. Ierosinājuma 5. pants pretēji šādām vērtībām riskē pieminēt "vērtības" un MI sistēmām aizliegto pretstatā šādām vērtībām. Patiešām 5. pantā minētie kritēriji MI sistēmu kā aizliegtu "kvalificēšanai" **ierobežo aizlieguma darbības jomu** tiktāl, ka praksē tas varētu izrādīties bezjēdzīgi (piemēram, "izraisa vai varētu izraisīt [...] fizisku vai psiholoģisku kaitējumu" saskaņā ar 5. panta 1. punkta (a) un (b) apakšpunktiem; ierobežojumu valsts iestādēm saskaņā ar 5. panta 1. punkta (c) apakšpunktu; neskaidru formulējumu (i) un (ii) (c) apakšpunktā; "reāllaika" attālās biometriskās identifikācijas ierobežojumu tikai bez skaidras definīcijas utt.).

29. Jo īpaši MI izmantošana "sociālai vērtēšanai", kā paredzēts Ierosinājuma 5. panta 1. punkta (c) apakšpunktā, var izraisīt diskrimināciju un ir pretrunā ES pamatvērtībām. Ierosinājums aizliedz šādu praksi tikai tad, ja tā tiek veikta "noteiktā laikposmā" vai arī to veic "valsts sektora iestādes vai to vārdā". Privāti uzņēmumi, jo īpaši sociālie tīkli un mākoņpakalpojumu sniedzēji, var apstrādāt lielus personas datu apjomus un veikt sociālo vērtēšanu. Līdz ar to **Ierosinājumā būtu jāaizliedz jebkāda veida sociālā vērtēšana**. Jāatzīmē, ka tiesībaizsardzības kontekstā LED 4. pants jau būtiski ierobežo — ja pat praktiski neaizliedz — šāda veida darbības.

30. Fizisku personu **attālināta biometriskā identifikācija** publiski pieejamās telpās rada lielu risku iejaukties fizisku personu privātajā dzīvē. Tāpēc EDAK un EDAU **uzskata, ka ir nepieciešama stingrāka pieeja**. MI sistēmu izmantošana var radīt nopietnas

proporcionalitātes problēmas, jo var ietvert neizvēlīga un nesamērīga skaita datu subjektu datu apstrādi, lai identificētu tikai dažas personas (piemēram, pasažierus lidostās un dzelzceļa stacijās). Attālināto biometrisko identifikācijas sistēmu **netraucētais** raksturs nozīmē arī pārredzamības problēmas saistībā ar apstrādes juridisko pamatu atbilstoši ES tiesību aktiem (LED, VDAR, EUDPR un citi piemērojamie tiesību akti). Joprojām nav atrisināta problēma par veidu, kā pienācīgi informēt fiziskās personas par šo apstrādi, kā arī efektīva un savlaicīga fizisko personu tiesību izmantošana. Tas pats attiecas uz **tās neatgriezenisko, smago ietekmi uz iedzīvotāju** (pamatotajām) **cerībām uz anonimitāti publiskās telpās**, kas tiešā veidā negatīvi ietekmē vārda, pulcēšanās, biedrošanās un pārvietošanās brīvības izmantošanu.

31. Ierosinājuma 5. panta 1. punkta (d) apakšpunktā ir sniegts plašs **ārkārtas gadījumu saraksts**, kad tiesībaizsardzības nolūkos ir atļauta "reāllaika" attālināta biometriskā identifikācija publiski pieejamās vietās. EDAK un EDAU uzskata **šo pieeju par kļūdainu** vairākos aspektos: Pirmkārt, nav skaidrs, kas būtu jāsaprot ar "ievērojamu aizkavi" un kā tas jāuzskata par atbildību mīkstinošu apstākli, ņemot vērā, ka masveida identifikācijas sistēma spēj identificēt tūkstošiem fizisku personu tikai dažu stundu laikā. Turklāt apstrādes uzmācība ne vienmēr ir atkarīga no tā, vai identifikācija tiek veikta reāllaikā. Pēc attālinātās biometriskās identifikācijas politiskā protesta kontekstā, iespējams, būs ievērojama atvēsinoša ietekme uz pamattiesību un brīvību izmantošanu, piemēram, pulcēšanās un biedrošanās brīvību un demokrātijas pamatprincipiem kopumā. Otrkārt, apstrādes uzmācība ne vienmēr ir atkarīga no tās mērķa. Šīs sistēmas izmantošana citiem nolūkiem, piemēram, privātai drošībai, rada tādus pašus apdraudējumus pamattiesībām uz privāto un ģimenes dzīvi un personas datu aizsardzībai. Visbeidzot, pat ņemot vērā paredzētos ierobežojumus, kriminālnoziegumos aizdomās turēto vai vainīgo iespējamais skaits gandrīz vienmēr būs "pietiekami liels", lai attaisnotu MI sistēmu nepārtrauktu izmantošanu aizdomās turamo atklāšanai, neraugoties uz turpmākajiem nosacījumiem Ierosinājuma 5. panta 2.–4. punktā. Ierosinājuma pamatojumā, šķiet, nav minēts, ka, uzraugot atklātas zonas, ir jāievēro ES datu aizsardzības tiesību aktos noteiktās saistības ne tikai attiecībā uz aizdomās turamajiem, bet arī uz visiem tiem, kuri praksē tiek uzraudzīti.

32. Šo iemeslu dēļ EDAK un EDAU **aicina noteikt vispārēju aizliegumu MI izmantošanai, lai automatizēti atpazītu cilvēka iezīmes publiski pieejamās vietās — piemēram, sejas, bet arī gaitu, pirkstu nospiedumus, DNS, balsi, taustiņsitienus un citus biometriskus vai uzvedības signālus, turklāt jebkurā kontekstā**. Ierosinājuma pašreizējā pieeja paredz identificēt un uzskaitīt visas MI sistēmas, kuras būtu jāaizliedz. Tādējādi konsekvences labad **MI sistēmas liela mēroga attālinātai identifikācijai tiešsaistes telpās** būtu jāaizliedz saskaņā ar Ierosinājuma 5. pantu. Ņemot vērā LED, EUDPR un VDAR, EDAU un EDAK nevar saskatīt, kā šāda veida prakse varētu atbilst nepieciešamības un proporcionalitātes principa prasības un kā visbeidzot izriet no tā, ko EST un ECT uzskata par pieņemamu iejaukšanos pamattiesībās.

33. Turklāt EDAK un EDAU **iesaka** gan valsts iestādēm, gan privātām struktūrām aizliegt **MI sistēmas, kas fiziskas personas pēc biometrijas (piemēram, pēc sejas atpazīšanas) klasificē grupās — pēc etniskās piederības, dzimuma, kā arī politiskās vai seksuālās orientācijas vai citiem diskriminācijas pamatiem, kas ir aizliegti saskaņā ar Hartas 21. pantu, un** MI

sistēmas, kuru zinātniskais pamatojums nav pierādīts vai kuras ir tiešā pretrunā ar ES pamatvērtībām (piemēram, poligrāfs, III pielikuma 6. panta (b) apakšpunkts un 7. panta (a) apakšpunkts). Attiecīgi "**biometrisko kategoriju noteikšana**" būtu **jāaizliedz saskaņā ar 5. pantu**.

34. Turklāt tas **ietekmē cilvēka cieņu, ko dators nosaka vai klasificē attiecībā uz turpmāko uzvedību neatkarīgi no paša cilvēka brīvas gribas**. MI sistēmas, kas ir paredzētas tiesībaizsardzības iestāžu izmantošanai, veicot fizisku personu individuālus riska novērtējumus, lai novērtētu fiziskas personas risku atkārtoti iesaistīties noziedzīgos nodarījumos, pam. III pielikuma 6. panta (a) apakšpunkts, vai prognozētu faktiska vai iespējama noziedzīga nodarījuma atgadījumu vai atkārtošanos, pamatojoties uz fiziskas personas profilēšanu vai personības iezīmju un īpašību vai pagātnes noziedzīgas rīcības novērtēšanu, pam. III pielikuma 6. panta (e) apakšpunkts, izmantojot atbilstoši paredzētajam nolūkam, virzīs uz policijas un tiesu lēmumu pieņemšanas izšķirošu pakļautību, tādējādi objektivizējot ietekmēto cilvēku. Šādas MI sistēmas, kas skar tiesību uz cilvēka cieņu būtību, ir jāaizliedz saskaņā ar 5. pantu.

35. Turklāt EDAK un EDAU uzskata, ka MI izmantošana, lai **secinātu fiziskas personas emocijas, ir ļoti nevēlama un būtu jāaizliedz**, izņemot dažus precīzi noteiktus lietošanas gadījumus, proti, veselības vai pētniecības nolūkos (piemēram, pacientiem, kuriem ir svarīga emociju atpazīšana), vienmēr īstenojot atbilstīgus aizsardzības pasākumus un, protams, ievērojot visus citus datu aizsardzības nosacījumus un ierobežojumus, tostarp mērķa ierobežojumus.

2.4 Augsta riska MI sistēmas

2.4.1 Ārēju trešo pušu *ex-ante* atbilstības novērtēšanas nepieciešamība

36. EDAK un EDAU atzinīgi vērtē to, ka MI sistēmas, kas rada augstu risku, ir jānovērtē, pirms tās var laist tirgū vai kā citādi nodot ekspluatācijā ES. Principā šis normatīvais modelis ir apsveicams, jo tas piedāvā labu līdzsvaru starp labvēlīgu attieksmi pret inovācijām un augstu proaktīvas pamattiesību aizsardzības līmeni. Lai to varētu izmantot īpašā vidē, piemēram, sabiedrisko pakalpojumu iestāžu vai kritiskas infrastruktūras lēmumu pieņemšanas procesos, ir jānosaka veidi, kā izpētīt visu pirmkodu.

37. Tomēr EDAK un EDAU iestājas par atbilstības novērtēšanas procedūras pielāgošanu saskaņā ar Ierosinājuma 43. pantu tādā veidā, ka **augsta riska MI parasti ir jāveic *ex ante* trešās puses atbilstības novērtēšana.** Lai gan trešās puses atbilstības novērtēšana augsta riska personas datu apstrādei nav prasība no VDAR vai EUDPR, MI sistēmu radītie riski vēl ir pilnībā jāizprot. Tādējādi pienākuma vispārēja iekļaušana trešās puses atbilstības novērtēšanā vēl vairāk stiprinātu juridisko noteiktību un uzticēšanos visām augsta riska MI sistēmām.

2.4.2 Regulas darbības jomai ir jāaptver arī jau izmantotās MI sistēmas

38. Saskaņā ar Ierosinājuma 43. panta 4. punktu augsta riska MI sistēmām jauna atbilstības novērtēšanas procedūra būtu jāpiemēro ikreiz, kad tiek veiktas būtiskas izmaiņas. Pareizi būtu nodrošināt MI sistēmu atbilstību MI regulas prasībām visā to dzīves ciklā. MI sistēmas, kas ir

izlaistas tirgū vai nodotas ekspluatācijā pirms ierosinātās regulas piemērošanas (vai 12 mēnešus pēc tam IX pielikumā uzskaitītajām liela mēroga IT sistēmām), nav iekļautas to darbības jomā, ja vien šīs sistēmas netiek pakļautas "būtiskām izmaiņām" attiecībā uz konstrukciju vai paredzēto mērķi (83. pants).

39. Tomēr "būtisku izmaiņu" slieksnis ir neskaidrs. Ierosinājuma 66. apsvērumā kā zemākais slieksnis ir noteikta atbilstības atkārtota novērtēšana "ikreiz, kad notiek izmaiņas, kas var ietekmēt atbilstību". Līdzīgs slieksnis būtu piemērots 83. pantam, uz augsta riska MI sistēmām. Turklāt, lai novērstu jebkādas aizsardzības nepilnības, ir nepieciešams, lai MI sistēmas, kas jau ir izveidotas un darbojas — pēc noteiktas ieviešanas fāzes, atbilstu visām MI regulas prasībām.

40. Personas datu apstrādes daudzkārtīgās iespējas un ārējie riski ietekmē arī MI sistēmu drošību. 83. pantā uzsvars uz "būtiskām konstrukcijas vai paredzētā nolūka izmaiņām" neiekļauj atsauci uz ārējo risku izmaiņām. Tāpēc Ierosinājuma 83. pantā ir jāiekļauj atsauce uz izmaiņām apdraudējuma scenārijā, ko rada ārēji riski, piemēram, kiberuzbrukumi, pretinieku uzbrukumi un pamatotas patērētāju sūdzības.

41. Turklāt, tā kā piemērošana ir paredzēta 24 mēnešus pēc jaunās regulas stāšanās spēkā, EDAU un EDAK neuzskata par piemērotu attiecināt izņēmumu par ilgāku laika periodu uz MI sistēmām, kas jau ir izlaistas tirgū. Lai gan Ierosinājumā ir arī paredzēts, ka Regulas prasības ir jāņem vērā, novērtējot katru liela mēroga IT sistēmu, kā noteikts IX pielikumā uzskaitītajos tiesību aktos, EDAK un EDAU uzskata, ka prasības attiecībā uz MI sistēmu nodošanu ekspluatācijā būtu jāpiemēro no jaunās Regulas piemērošanas dienas.

2.5 Pārvalde un Eiropas MI padome

2.5.1 Pārvaldība

42. EDAK un EDAU atzinīgi vērtē EDAU izraudzīšanu par kompetento iestādi un tirgus uzraudzības iestādi Savienības iestāžu, aģentūru un struktūru uzraudzībai, ja uz tām attiecas šis Ierosinājums. EDAU ir gatavs pildīt savu jauno uzdevumu kā ES valsts pārvaldes MI regulators. Turklāt EDAU loma un uzdevumi nav pietiekami detalizēti un būtu sīkāk jāprecizē Ierosinājumā, jo īpaši attiecībā uz tā kā tirgus uzraudzības iestādes lomu.

43. Ierosinājumā EDAK un EDAU atzīst finanšu resursu piešķiršanu, kas ierosinājumā ir paredzēti Valdei un EDAU, kas darbojas kā ziņojošā struktūra. Tomēr EDAU paredzēto jauno pienākumu izpilde neatkarīgi no tā, vai tas veic paziņotās struktūras pienākumus, prasītu ievērojami lielākus finanšu un cilvēkresursus.

44. Pirmkārt, tāpēc, ka 63. panta 6. punkta formulējumā ir teikts, ka EDAU "ir jārīkojas kā tirgus uzraudzības iestādei" attiecībā uz Savienības iestādēm, aģentūrām un struktūrām, kas ietilpst Ierosinājuma darbības jomā, un nav precizēts, vai EDAU ir jāuzskata par pilnībā iemiesotu "tirgus uzraudzības iestādi", kā paredzēts Regulā (ES) 2019/1020. Tas rada jautājumus par EDAU pienākumiem un pilnvarām praktiskajā darbībā. Otrkārt, ar nosacījumu, ka atbilde uz pirmo jautājumu ir apstiprinoša, nav skaidrs, kā EDAU loma, kā paredzēts EUDPR, var izpildīt uzdevumu, kas ir paredzēts Regulas (ES) 2019/1020 11. pantā un iekļauj "efektīvu tirgus uzraudzību savā teritorijā attiecībā uz tiešsaistē pieejamiem produktiem"vai "fiziskas un

laboratoriskas pārbaudes, pamatojoties uz atbilstošiem paraugiem". Pastāv risks, ka jaunā uzdevumu kopuma uzņemšanās bez sīkākiem precizējumiem Ierosinājumā var apdraudēt tā kā datu aizsardzības uzraudzītāja pienākumu izpildi.

45. Tomēr EDAK un EDAU uzsver, ka dažu Ierosinājuma noteikumu, kas definē dažādu kompetento iestāžu uzdevumus un pilnvaras saskaņā ar MI regulu, attiecības, raksturs un neatkarības garantija šajā posmā šķiet neskaidri. Tā kā Regulā 2019/1020 ir noteikts, ka tirgus uzraudzības iestādei ir jābūt neatkarīgai, regulas projektā netiek prasīts, lai uzraudzības iestādes būtu neatkarīgas, un pat tiek prasīts, lai tās ziņotu Komisijai par dažiem uzdevumiem, ko veic tirgus uzraudzības iestādes, kas var būt atšķirīgas struktūras. Tā kā ierosinājumā ir arī noteikts, ka DAI būs tiesībaizsardzības nolūkos (63. panta 5. punkts) izmantoto MI sistēmu tirgus uzraudzības iestādes, tas nozīmē arī to, ka, iespējams, ar savas valsts uzraudzības iestādes starpniecību tām būs pienākums ziņot Komisijai (63. panta 2. punkts), un tas, šķiet, nav savienojams ar šo struktūru neatkarību.

46. Tāpēc EDAK un EDAU uzskata, ka šie noteikumi ir jāprecizē, lai tie atbilstu Regulai 2019/1020, EUDPR un VDAR, turklāt Ierosinājumā ir skaidri jānosaka, ka Uzraudzības iestādēm saskaņā ar MI regulu ir jābūt pilnīgi neatkarīgām uzdevumu izpildē, jo tā būtu būtiska garantija pienācīgai uzraudzībai un jaunās Regulas izpildei.

47. Turklāt EDAK un EDAU vēlētos atgādināt, ka datu aizsardzības iestādes (DAI) jau īsteno VDAR, EUDPR un LED MI sistēmās, kas ietver personas datus, lai nodrošinātu aizsardzību pamattiesībām un jo īpaši tiesībām uz datu aizsardzību. Tāpēc, kā pieprasīts Ierosinājumā par valstu uzraudzības iestādēm, DAI jau ir zināma izpratne par MI tehnoloģijām, datiem un datu skaitļošanu, pamattiesībām un zinātība par jauno tehnoloģiju radīto pamattiesību risku novērtēšanu. Turklāt, ja MI sistēmu pamatā ir personas datu apstrāde vai tās apstrādā personas datus, Ierosinājuma noteikumi ir tieši saistīti ar datu aizsardzības tiesisko regulējumu, kas attieksies uz lielāko daļu no regulas darbības jomas MI sistēmām. Līdz ar to pastāvēs savstarpējas kompetenču saistības starp uzraudzības iestādēm, uz kurām attiecas Ierosinājums, un DAI.

48. Tādējādi DAI izraudzīšana par valsts uzraudzības iestādēm nodrošinātu saskaņotāku regulatīvo pieeju, palīdzētu konsekventi interpretēt datu apstrādes noteikumus un novērstu pretrunas to izpildē starp dalībvalstīm. Būtu arī izdevīgi visām MI vērtību ķēdes ieinteresētajām personām izveidot vienu kontaktpunktu visām personas datu apstrādes darbībām, kas ietilpst Ierosinājuma darbības jomā, un ierobežot mijiedarbību starp divām dažādām apstrādes regulatīvajām iestādēm, uz kurām attiecas Ierosinājums un VDAR. Līdz ar to EDAK un EDAU uzskata, ka **DAI būtu jāieceļ par valsts uzraudzības iestādēm saskaņā ar Ierosinājuma 59. pantu.**

49. Jebkurā gadījumā, ciktāl Ierosinājumā ir iekļauti īpaši noteikumi par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, kas pieņemti, pamatojoties uz LESD 16. pantu, šo noteikumu ievērošana, jo īpaši par MI sistēmu izmantošanas ierobežojumiem reāllaikā attālinātai biometriskai identifikācijai publiski pieejamās vietās tiesībaizsardzības nolūkos, **ir jābūt pakļautai neatkarīgu iestāžu kontrolei**.

50. Tomēr Ierosinājumā nav skaidra noteikuma, lai piešķirtu kompetenci šo noteikumu ievērošanas nodrošināšanai neatkarīgu iestāžu kontrolē. Vienīgā atsauce uz kompetentajām datu aizsardzības uzraudzības iestādēm saskaņā ar VDAR jeb LED ir Ierosinājuma 63. panta 5. punktā, bet tikai kā "tirgus uzraudzības" struktūras un alternatīva dažām citām iestādēm. EDAK un EDAU uzskata, ka šī struktūra nenodrošina atbilstību LESD 16. panta 2. punktā un Hartas 8. pantā noteiktajai neatkarīgas kontroles prasībai.

2.5.2 Eiropas MI padome

51. Ar Ierosinājumu tiek izveidota "Eiropas Mākslīgā intelekta padome" (EAIB). EDAK un EDAU atzīst nepieciešamību konsekventi un saskaņoti piemērot ierosināto saturu, kā arī iesaistīt neatkarīgus ekspertus ES politikas izstrādē attiecībā uz MI. Tajā pašā laikā Ierosinājums paredz dominējošās lomas piešķiršanu Komisijai. Tādējādi Komisija ne tikai būtu EAIB daļa, bet arī to vadītu un tai būtu veto tiesības EAIB reglamenta pieņemšanā. Tas ir pretrunā ar MI Eiropas struktūras nepieciešamību būt neatkarīgai no jebkādas politiskas ietekmes. Tāpēc EDAK un EDAU uzskata, ka jaunajai MI regulai būtu jāpiešķir **EAIB lielāka autonomija**, lai tā varētu patiesi nodrošināt regulas konsekventu piemērošanu visā vienotajā tirgū.

52. EDAK un EDAU arī norāda, ka EAIB netiek piešķirtas nekādas pilnvaras attiecībā uz ierosinātās Regulas izpildi. Tomēr, ņemot vērā MI sistēmu izplatību vienotajā tirgū un pārrobežu gadījumu iespējamību, ir ārkārtīgi nepieciešama saskaņota izpilde un pienācīga kompetences sadale starp valstu uzraudzības iestādēm. Tāpēc EDAK un EDAU iesaka jaunajā MI regulā precizēt valstu uzraudzības iestāžu sadarbības mehānismus. EDAK un EDAU ierosina ieviest mehānismu, kas garantē vienotu kontaktpunktu personām, uz kurām attiecas tiesību akti, kā arī uzņēmumiem, katrai MI sistēmai, un to, ka attiecībā uz organizācijām, kuru darbība aptver vairāk nekā pusi no ES dalībvalstīm, EAIB var izraudzīties valsts iestādi, kas būs atbildīga par MI regulas izpildi attiecībā uz šo MI sistēmu.

53. Turklāt, ņemot vērā Padomes sastāvu veidojošo iestāžu neatkarīgo raksturu, tā ir tiesīga rīkoties pēc savas iniciatīvas, nevis tikai sniegt padomus un palīdzību Komisijai. Tāpēc EDAK un EDAU uzsver nepieciešamību pagarināt Padomes misiju, kas turklāt neatbilst Ierosinājumā uzskaitītajiem uzdevumiem.

54. Lai sasniegtu šos mērķus, **EAIB ir jābūt pietiekamām un atbilstošām pilnvarām**, un ir jāprecizē tās juridiskais statuss. Jo īpaši, lai jaunās regulas materiālā piemērošanas joma paliktu aktuāla, šķiet nepieciešams tās izstrādē iesaistīt par tās piemērošanu atbildīgās iestādes. Tādējādi EDAK un EDAU iesaka piešķirt EAIB pilnvaras, lai ierosinātu Komisijai grozījumus I pielikumā, definējot MI metodes un pieejas, un III pielikumā, kurā ir uzskaitītas 6. panta 2. punktā minētās augsta riska MI sistēmas. Pirms izdarīt jebkādus grozījumus šajos pielikumos, Komisijai ir jākonsultējas arī ar EAIB.

55. Ierosinājuma 57. panta 4. punkts paredz apmaiņu starp Padomi un citām Savienības struktūrām, birojiem, aģentūrām un padomdevēju grupām. Ņemot vērā viņu iepriekšējo darbu MI jomā un pieredzi cilvēktiesību jomā, EDAK un EDAU iesaka uzskatīt Pamattiesību aģentūru par vienu no Padomes novērotājiem.

3 MIJIEDARBĪBA AR DATU AIZSARDZĪBAS STRUKTŪRU

3.1 Ierosinājuma saistība ar spēkā esošajiem ES datu aizsardzības tiesību aktiem

56. Skaidri definēta sakarība starp Ierosinājumu un spēkā esošajiem datu aizsardzības tiesību aktiem ir būtisks priekšnosacījums, lai nodrošinātu un saglabātu cieņu un ES acquis ievērošanu un piemērošanu personas datu aizsardzības jomā. Šādi ES tiesību akti, jo īpaši VDAR, EUDPR un LED, ir jāuzskata par priekšnosacījumu, uz kuru var balstīties turpmākie likumdošanas ierosinājumi, neietekmējot esošos noteikumus vai netraucējot tiem, tostarp attiecībā uz uzraudzības iestāžu kompetenci un pārvaldību.

57. Tāpēc, ņemot vērā EDAK un EDAU, ir svarīgi Ierosinājumā skaidri izvairīties no jebkādas pretrunas un iespējamiem konfliktiem ar VDAR, EUDPR un LED. Tas ir ne tikai juridiskās noteiktības labad, bet arī tāpēc, lai izvairītos no tā, ka Ierosinājums tieši vai netieši apdraud pamattiesības uz personas datu aizsardzību, kā noteikts LESD 16. pantā un Hartas 8. pantā.

58. Jo īpaši pašmācības iekārtas varētu aizsargāt fizisku personu personas datus tikai tad, ja tas ir iestrādāts koncepcijā. Būtiska ir arī tūlītēja iespēja izmantot fizisku personu tiesības saskaņā ar VDAR 22. pantu (Automātiska individuālu lēmumu pieņemšana, iekļaujot profilēšanu) vai EUDPR 23. pantu neatkarīgi no apstrādes nolūkiem. Šajā ziņā MI sistēmās jau no paša sākuma ir jānodrošina citas datu subjektu tiesības, kas ir saistītas ar dzēšanas tiesībām un tiesībām veikt labojumus saskaņā ar datu aizsardzības tiesību aktiem, neatkarīgi no izvēlētās MI pieejas vai tehniskās arhitektūras.

59. Izmantojot personas datus MI sistēmu apgūšanai, MI sistēmas pamatā var būt neobjektīvi lēmumu pieņemšanas modeļi. Tādējādi, lai nodrošinātu datu subjektu tiesību ievērošanu un garantēšanu, kā arī izvairītos no jebkādas negatīvas ietekmes uz fiziskām personām, būtu jāpieprasa dažādi aizsardzības pasākumi un jo īpaši kvalificēta cilvēku uzraudzība šādos procesos. Turklāt kompetentajām iestādēm vajadzētu būt iespējai ierosināt vadlīnijas, lai novērtētu neobjektivitāti MI sistēmās un palīdzētu veikt cilvēku uzraudzību.

60. Ja datu subjektu dati tiek izmantoti MI apmācībai un/vai prognozēšanai, viņi vienmēr būtu jāinformē par šādas apstrādes juridisko pamatu, vispārēju MI sistēmas loģikas (procedūras) un darbības jomas skaidrojumu. Šajā saistībā vienmēr būtu jāgarantē indivīdu tiesības uz apstrādes ierobežošanu (VDAR 18. pants un EUDPR 20. pants), kā arī datu dzēšanu (VDAR 16. pants un EUDPR 19. pants). Turklāt pārzinim vajadzētu būt nepārprotamam pienākumam informēt datu subjektu par piemērojamajiem termiņiem iebildumu iesniegšanai, ierobežošanai, datu dzēšanai utt. MI sistēmai ir jāspēj izpildīt visas datu aizsardzības prasības, veicot atbilstošus tehniskus un organizatoriskus pasākumus. Tiesībām uz skaidrojumu vajadzētu nodrošināt papildu pārredzamību.

3.2 Smilškaste un turpmāka apstrāde (Ierosinājuma 53. un 54. pants)

61. Ievērojot esošās juridiskās un morālās robežas, ir svarīgi veicināt Eiropas inovāciju, izmantojot tādus rīkus kā smilškaste. Smilškaste sniedz iespēju nodrošināt drošības pasākumus, kas ir nepieciešami, lai radītu uzticību un paļaušanos uz MI sistēmām. Sarežģītā vidē MI praktiķiem

var būt grūti pareizi izsvērt visas intereses. It īpaši maziem un vidējiem uzņēmumiem ar ierobežotiem resursiem darbība regulējumu izmēģināšanas režīmā var sniegt ātrāku ieskatu un tādējādi veicināt inovāciju.

62. Ierosinājuma 53. panta 3. iedaļā teikts, ka izmēģināšanas režīmā neietekmē uzraudzības un korekciju pilnvaras. Ja šis skaidrojums ir noderīgs, ir arī jāizstrādā norādījumi vai vadlīnijas par to, kā panākt labu līdzsvaru starp uzraudzības iestādes lomu, no vienas puses, un sniegt detalizētus norādījumus, izmantojot izmēģināšanas režīmu, no otras puses.

63. 53. panta 6. sadaļā ir aprakstīts, ka izmēģināšanas režīma darbības kārtību un nosacījumus nosaka īstenošanas aktos. Svarīgi ir izstrādāt īpašas nostādnes, lai nodrošinātu konsekvenci un atbalstu izmēģināšanas režīmu izveidē un darbībā. Tomēr saistoši īstenošanas akti varētu ierobežot katras dalībvalsts iespējas pielāgot izmēģināšanas režīmu atbilstoši savām vajadzībām un vietējai praksei. Tādējādi EDAK un EDAU iesaka EAIB tā vietā sniegt nostādnes izmēģinājuma režīmiem.

64. Ierosinājuma 54. panta mērķis ir nodrošināt juridisku pamatu personas datu turpmākai apstrādei, lai izstrādātu noteiktas MI sistēmas sabiedrības interesēs MI reglamentējumu izmēģināšanas režīmā. Ierosinājuma 54. panta 1. punkta saistība ar Ierosinājuma 54. panta 2. apakšpunktu un 41. apsvērumu un līdz ar to arī esošajiem ES datu aizsardzības tiesību aktiem paliek neskaidra. Tomēr VDAR un EUDPR jau ir izveidots pamats turpmākai apstrādei. Jo īpaši attiecībā uz gadījumiem, kad sabiedrības interesēs ir atļaut turpmāku apstrādi, līdzsvaram starp pārziņa un datu subjekta interesēm nav jākavē inovācijas. Ierosinājuma 54. pantā pašlaik nav aplūkoti divi svarīgi jautājumi: i) kādos apstākļos un pēc kādiem (papildu) kritērijiem tiek izsvērtas datu subjektu intereses; ii) vai šīs MI sistēmas tiks izmantotas tikai izmēģinājuma režīmā. EDAK un EDAU atzinīgi vērtē prasību pēc Savienības vai Dalībvalsts tiesību aktiem, apstrādājot personas datus, kas ir savākti LED zmēģinājuma režīmā, bet iesaka sīkāk precizēt šeit paredzēto VDAR un EUDPR atbilstošā veidā, galvenokārt precizējot, ka šādu izmēģinājuma režīmu juridiskajam pamatam ir jāatbilst VDAR 23. panta 2. punktā un EUDPR 25. pantā noteiktajām prasībām un katra izmēģinājuma režīma izmantošana ir rūpīgi jāizvērtē. Tas attiecas arī uz pilnu nosacījumu sarakstu no 54. panta 1. punkta (no b līdz j apakšpunktam).

65. Daži papildu apsvērumi par datu atkārtotu izmantošanu Ierosinājuma 54. pantā norāda, ka izmēģinājuma režīma lietošana ir resursietilpīga, un tāpēc ir reāli uzskatīt, ka tur varētu piedalīties tikai neliels skaits uzņēmumu. Dalība izmēģinājuma režīmā varētu būt konkurences priekšrocība. Lai ļautu atkārtoti izmantot datus, būtu rūpīgi jāapsver, kā atlasīt dalībniekus, lai pārliecinātos, vai viņi ietilpst darbības jomā, un izvairītos no negodīgas attieksmes. EDAK un EDAU pauž bažas, ka datu atkārtotas izmantošanas iespēja izmēģinājuma režīma ietvaros atšķiras no VDAR pārskatatbildības pieejas, kur pārskatatbildība tiek piemērota datu pārzinim, nevis kompetentajai iestādei.

66. Turklāt EDAK un EDAU uzskata, ka, ņemot vērā izmēģinājuma režīma mērķus, kas ir MI sistēmu izstrāde, pārbaude un apstiprināšana, izmēģinājuma režīmus nevar iekļaut LED darbības jomā. Lai gan LED paredz datu atkārtotu izmantošanu zinātniskiem pētījumiem, šim sekundārajam nolūkam apstrādātie dati tiks pakļauti VDAR vai EUDPR, nevis LED.

67. Nav skaidrs, ko ietvers regulējumu izmēģinājuma režīms. Rodas jautājums, vai ierosinātais regulācijas izmēģinājuma režīms iekļauj IT infrastruktūru katrā Dalībvalstī ar papildu juridisku pamatu turpmākai apstrādei vai arī tikai organizē piekļuvi regulatīvajām zināšanām un norādījumiem. EDAK un EDAU mudina likumdevēju precizēt šo jēdzienu Ierosinājumā un tur skaidri norādīt, ka regulācijas izmēģinājuma režīms neietver pienākumu kompetentajām iestādēm nodrošināt savu tehnisko infrastruktūru. Jebkurā gadījumā finanšu un cilvēkresursi ir jānodrošina kompetentajām iestādēm atbilstoši šādam skaidrojumam.

68. Visbeidzot EDAK un EDAU vēlētos uzsvērt tādu pārrobežu MI sistēmu izstrādi, kas būs pieejamas Eiropas digitālajam vienotajam tirgum kopumā. Šādu MI sistēmu gadījumā regulācijas smilškastei kā inovācijas instrumentam nevajadzētu kļūt par šķēršli pārrobežu attīstībai. Tāpēc EDAK un EDAU iesaka koordinētu pārrobežu pieeju, kas valsts līmenī joprojām ir pietiekami pieejama visiem MVU, piedāvājot vienotu sistēmu visā Eiropā, kas vienlaikus nav pārāk ierobežojoša. Jāpanāk līdzsvars starp Eiropas koordināciju un valstu procedūrām, lai izvairītos no jaunās MI regulas pretrunīgas ieviešanas, kas kavētu inovācijas visā ES.

3.3 Pārredzamība

69. EDAK un EDAU atzinīgi vērtē to, ka augsta riska MI sistēmas ir jāreģistrē publiskā datu bāzē (minēts Ierosinājuma 51. un 60. pantā). Šī datu bāze būtu jāizmanto kā iespēja plašai sabiedrībai sniegt informāciju par MI sistēmas lietojuma piemērošanas jomu, kā arī zināmajām nepilnībām un starpgadījumiem, kas varētu apdraudēt to darbību, un pakalpojumu sniedzēju pieņemtajiem līdzekļiem to noteikšanai un novēršanai.

70. Svarīgs demokrātijas princips ir līdzsvara un atsvara sistēmas izmantošana. Tāpēc fakts, ka pārredzamības pienākums neattiecas uz MI sistēmām, ko izmanto noziedzīgu nodarījumu atklāšanai, novēršanai, izmeklēšanai vai saukšanai pie atbildības, ir pārāk plašs izņēmums. Jānošķir MI sistēmas, ko izmanto, lai atklātu vai novērstu, un MI sistēmas, kuru mērķis ir izmeklēt, lai palīdzētu noziedzīgu nodarījumu izmeklēšanā. Profilakses un atklāšanas aizsardzības pasākumiem ir jābūt stingrākiem nevainīguma prezumpcijas dēļ. Turklāt EDAK un EDAU pauž nožēlu, ka ierosinājumā nav brīdinājumu, ko var interpretēt kā zaļo gaismu pat nepierādītu, augsta riska MI sistēmu vai lietojumu izmantošanai.

71. Gadījumos, kad sabiedrībai slepenības apsvērumu dēļ pat labi funkcionējošā demokrātijā, var nodrošināt mazu pārredzamību vai tās nav vispār, ir jāievieš drošības pasākumi un šīs MI sistēmas jāreģistrē kompetentajā uzraudzības iestādē un jānodrošina tai pārredzamība.

72. Pārredzamības nodrošināšana MI sistēmās ir ļoti izaicinošs mērķis. Pilnībā kvantitatīva daudzu MI sistēmu lēmumu pieņemšanas pieeja, kas pēc būtības atšķiras no cilvēka pieejas, galvenokārt balstoties uz cēloņsakarību un teorētisku pamatojumu, var būt pretrunā ar nepieciešamību iepriekš iegūt saprotamu mašīnu rezultātu skaidrojumu. Regulai vajadzētu veicināt jaunus, proaktīvākus un savlaicīgākus veidus, kā informēt MI sistēmu lietotājus par (lēmumu pieņemšanas) statusu, kurā sistēma atrodas jebkurā laikā, sniedzot agrīnu brīdinājumu par iespējamiem kaitīgiem iznākumiem, lai personas, kuru tiesības un brīvības varētu būt traucētas mašīnas autonomo lēmumu dēļ, varētu reaģēt vai labot lēmumu.

3.4 Īpašu kategoriju datu un datu, kas saistīti ar noziedzīgiem nodarījumiem, apstrāde

73. Īpašu kategoriju datu apstrādi tiesībaizsardzības jomā reglamentē ES datu aizsardzības sistēmas noteikumi, tostarp LED, kā arī to īstenošana valstī. Ierosinājumā ir apgalvots, ka tas nenodrošina vispārēju juridisku pamatu personas datu apstrādei, iekļaujot īpašas personas datu kategorijas, pam. 41. apsvērums. Tajā pašā laikā Ierosinājuma 10. panta 5. punktā ir norādīts, ka "šādu sistēmu nodrošinātāji var apstrādāt īpašas personas datu kategorijas". Turklāt tas pats noteikums prasa papildu aizsardzības pasākumus, sniedzot arī piemērus. Tādējādi šķiet, ka Ierosinājums traucē VDAR, LED un EUDPR piemērošanai. Lai gan EDAK un EDAU atzinīgi vērtē mēģinājumu nodrošināt atbilstošus aizsardzības pasākumus, ir nepieciešama saskaņotāka regulatīvā pieeja, jo pašreizējie noteikumi nešķiet pietiekami skaidri, lai izveidotu juridisku pamatu īpašu kategoriju datu apstrādei, un tie ir papildināti ar papildu aizsardzības pasākumiem, kas vēl jānovērtē. Turklāt, ja personas dati ir savākti, veicot apstrādi LED darbības jomā, būs jāņem vērā iespējamie papildu drošības pasākumi un ierobežojumi, kas izriet no LED transponēšanas valsts līmenī.

3.5 Atbilstības mehānismi

3.5.1 Sertifikācija

74. Viens no Ierosinājuma galvenajiem pīlāriem ir sertifikācija. Ierosinājumā izklāstītā sertifikācijas sistēma ir balstīta uz struktūru uzbūvi (ziņojošās iestādes / pilnvarotās iestādes / Komisija) un atbilstības novērtēšanas/sertifikācijas mehānismu, kas aptver obligātās prasības, kuras ir piemērojamas augsta riska MI sistēmām, un balstās uz Eiropas saskaņotajiem standartiem atbilstoši Regulai (ES) Nr. 1025/2012 un kopējām specifikācijām, kas ir jānosaka Komisijai. Šis mehānisms atšķiras no sertifikācijas sistēmas, kuras mērķis ir nodrošināt VDAR 42. un 43. pantā izklāstīto datu aizsardzības noteikumu un principu ievērošanu. Tomēr nav skaidrs, kā saskaņā ar Ierosinājumu pilnvaroto iestāžu izsniegtie sertifikāti var mijiedarboties ar datu aizsardzības sertifikātiem, zīmogiem un zīmēm, ko paredz VDAR, atšķirībā no tā, kas ir paredzēts citu veidu sertifikātiem (skatiet 42. panta 2. punktu par sertifikātiem, kas tiek izsniegti saskaņā ar Regulu (ES) 2019/881).

75. Ciktāl augsta riska MI sistēmas ir balstītas uz personas datu apstrādi vai apstrādā personas datus, lai pildītu savu uzdevumu, šīs neatbilstības var radīt juridisku nenoteiktību visām iesaistītajām struktūrām, jo tās var izraisīt situācijas, kurās MI sistēmas, kas ir sertificētas saskaņā ar Ierosinājumu un marķētas ar CE atbilstības marķējumu, tiklīdz tās ir laistas tirgū vai nodotas ekspluatācijā, var tikt izmantotas veidā, kas neatbilst datu aizsardzības noteikumiem un principiem.

76. Ierosinājumā trūkst skaidras saistības ar datu aizsardzības tiesību aktiem, kā arī citiem ES un Dalībvalstu tiesību aktiem, kas ir piemērojami katrai III pielikumā uzskaitītajai augsta riska MI sistēmas "jomai". Ierosinājumā jo īpaši būtu jāiekļauj iestrādātas datu minimizēšanas un datu aizsardzības principi kā viens no aspektiem, kas jāņem vērā pirms CE marķējuma iegūšanas, ņemot vērā augsta riska MI sistēmu iespējamo lielo iejaukšanos pamattiesībās, privātuma un personas datu aizsardzībā, kā arī nepieciešamību nodrošināt augsta līmeņa uzticēšanos MI

sistēmai. Tāpēc EDAK un EDAU iesaka grozīt Ierosinājumu tā, lai precizētu saistību starp sertifikātiem, kas tika izdoti saskaņā ar minēto Regulu, un datu aizsardzības sertifikātiem, plombām un zīmēm. Visbeidzot datu aizsardzības iestādēm būtu jāiesaistās saskaņotu standartu un vispārēju specifikāciju sagatavošanā un izveidē.

77. Saistībā ar Ierosinājuma 43. pantu, kas attiecas uz atbilstības novērtēšanu, 47. pantā noteiktā atkāpe no atbilstības novērtēšanas procedūras, šķiet, ir ļoti plaša, ietverot pārāk daudzus izņēmumus, piemēram, sabiedrības drošības vai dzīvības aizsardzības un cilvēku veselības, vides aizsardzības un galveno industrijas un infrastruktūras aktīvu aizsardzības ārkārtas iemeslus. Mēs ierosinātu likumdevējiem tos sašaurināt.

3.5.2 Rīcības kodeksi

78. Saskaņā ar Ierosinājuma 69. pantu Komisija un Dalībvalstis mudina un atvieglo rīcības kodeksa (CoC) izstrādi, kura mērķis ir veicināt MI sistēmu, kurām nav augsta riska, nodrošinātāju brīvprātīgu piemērošanu prasībām, kas ir piemērojamas augsta riska MI sistēmām, kā arī papildu prasībām. Saskaņā ar VDAR 78. apsvērumu EDAK un EDAU iesaka identificēt un definēt sinerģiju starp šiem instrumentiem un VDAR paredzētajiem rīcības kodeksiem, kas atbalsta datu aizsardzības ievērošanu. Šajā kontekstā ir svarīgi precizēt, vai personas datu aizsardzība ir jāuzskata par "papildu prasībām", kuras var risināt 69. panta 2. punktā minētās CoC. Turklāt ir svarīgi nodrošināt, lai "tehniskās specifikācijas un risinājumi", kuriem ir pievērsies CoC, atsaucoties uz 69. panta 1. punktu, un kuru mērķis ir veicināt atbilstību MI regulas projekta prasībām, nebūtu pretrunā ar VDAR un EUDPR noteikumiem un principiem. Ja, šādi rīkojoties, šos instrumentus ievēros MI sistēmas, kas nav augsta riska nodrošinātāji — ciktāl šādas sistēmas ir balstītas uz personas datu apstrādi vai apstrādā personas datus, lai izpildītu savu uzdevumu — , un tiek radīta pievienotā vērtība, tas nodrošinās, ka pārzinis un apstrādātāji, izmantojot šīs sistēmas, spēs izpildīt savus datu aizsardzības pienākumus.

79. Tajā pašā laikā uzticama MI tiesiskais regulējums tiktu papildināts ar CoC integrēšanu, lai veicinātu uzticēšanos šīs tehnoloģijas izmantošanai tādā veidā, kas ir droša un atbilst likumam, tostarp pamattiesību ievērošanai. Tomēr šo instrumentu uzbūve būtu jāstiprina, paredzot mehānismus, kuru mērķis ir pārbaudīt, vai šādi kodeksi nodrošina efektīvas "tehniskās specifikācijas un risinājumus" un nosaka noteikt "skaidrus mērķus un galvenos darbības rādītājus šo mērķu sasniegšanas novērtēšanai" kā attiecīgo kodeksu neatņemamas sastāvdaļas. Turklāt nav atsauces uz rīcības kodeksu (obligātajiem) uzraudzības mehānismiem, kas ir paredzēti, lai pārbaudītu, vai MI riska sistēmas, kuras nav augsta riska nodrošinātāji, ievēro to noteikumus, turklāt iespēja atsevišķiem pakalpojumu sniedzējiem izstrādāt (un pašiem īstenot) minētos kodeksus (skatiet skaidrojuma raksta 5.2.7. sadaļu) var vēl vairāk vājināt šo instrumentu efektivitāti un izpildāmību.

80. Visbeidzot EDAK un EDAU lūdz paskaidrojumus par to, kāda veida iniciatīvas Komisija var izstrādāt saskaņā ar Ierosinājuma 81. apsvērumu, "lai atvieglotu tehnisko šķēršļu samazināšanu, kas kavē pārrobežu datu apmaiņu MI attīstībai".

4 SECINĀJUMS

81. Lai gan EDAK un EDAU atzinīgi vērtē Komisijas Ierosinājumu un uzskata, ka šāda regula ir nepieciešama, lai garantētu ES pilsoņu un iedzīvotāju pamattiesību ievērošanu, viņi uzskata, ka Ierosinājums ir jāpielāgo vairākos jautājumos, lai nodrošinātu tā piemērojamību un efektivitāti.

82. Ņemot vērā Ierosinājuma sarežģītību, kā arī jautājumus, kuru risināšana ir tā mērķis, vēl ir daudz darāmā, līdz Ierosinājums varētu izveidot labi funkcionējošu tiesisko regulējumu, kas efektīvi papildina VDAR, aizsargājot cilvēka pamattiesības un vienlaikus veicinot inovācijas. EDAK un EDAU arī turpmāk būs pieejami, lai piedāvātu savu atbalstu šajā ceļā.

Briselē, 2021. gada 18. jūnijā

Eiropas Datu aizsardzības kolēģijas vārdā	Eiropas Datu aizsardzības uzraudzītāja vārdā
Priekšsēdētājs	Uzraudzītājs
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI