



Briselē, 2022. gada 12. septembrī
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

Starpiestāžu lieta:
2021/0106(COD)

JURIDISKĀ DIENESTA ATZINUMS ¹

Sūtītājs:	Juridiskais dienests
Temats:	Priekšlikums – Eiropas Parlamenta un Padomes Regula, kas nosaka saskaņotas normas mākslīgā intelekta jomā – LESD 114. un 16. pantā paredzēto juridisko pamatu atbilstība attiecībā uz tiesībaizsardzībai un tiesu iestādēm piemērojamiem noteikumiem

I. IEVADS

1. Ierosinātajā regulā ir paredzēti saskaņoti noteikumi par mākslīgā intelekta sistēmu ("AI sistēmas") laišanu tirgū un nodošanu ekspluatācijā Savienībā ("ierosinātā regula") ².

¹ Šajā dokumentā iekļauti juridiski atzinumi, kas ir aizsargāti saskaņā ar 4. panta 2. punktu Eiropas Parlamenta un Padomes Regulā (EK) Nr. 1049/2001 (2001. gada 30. maijs) par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem un kurus Eiropas Savienības Padome nav publiskojuši. Padome patur visas likumīgās tiesības attiecībā uz jebkuru neatļautu publikāciju.

² Dok. 8115/21.

2. Telesakaru un informācijas sabiedrības jautājumu darba grupas 2022. gada 7. aprīļa sanāksmē Padomes Juridiskais dienests ("PJD") puda viedokli jautājumā par ierosinātās regulas par mākslīgā intelekta sistēmām abu juridisko pamatu (LESD 16. un 114. pants) atbilstību. Sniegtie paskaidrojumi apstiprināja, ka LESD 16. un 114. pants ir pareizie juridiskie pamati priekšlikumam un ka LESD 87. panta 2. punkta izmantošana LESD 114. panta vietā nav piemērota. Pēc darba grupas lūguma šajā atzinumā ir rakstiski izklāstīts un plašāk izvērst Juridiskā dienesta pārstāvja paustais viedoklis, ar ko tas iepazīstināja minētajā sanāksmē.
3. *AI* sistēmas ir definētas ierosinātās regulas 3. panta 1. punktā. Kopumā tās atbilst noteikta veida programmatūrai. Ierosinātā regula attiecas gan uz sagādātājiem, kas *AI* sistēmas laiž tirgū, gan arī uz sagādātājiem, kas *AI* sistēmas nodod ekspluatācijā. Turklāt ierosinātā regula attiecas arī uz lietotājiem. Sagādātājs var būt fiziska vai juridiska persona vai publiskā sektora iestāde /struktūra, kura izstrādā vai liek izstrādāt *AI* sistēmu laišanai tirgū vai nodošanai ekspluatācijā ar savu vārdu vai preču zīmi. Lietotājs var būt jebkura fiziska vai juridiska persona, publiskā sektora iestāde, aģentūra vai jebkura cita struktūra, kas izmanto tās pārziņā esošu *AI* sistēmu.

4. Saskaņā ar 3. pantā ietvertajām definīcijām tiesībaizsardzības un tiesu iestādes varētu kvalificēties kā *AI* sistēmas sagādātājas un/vai lietotājas. *AI* sistēmas, kuru paredzētais nolūks, kā to definējis sagādātājs, ir tiesībaizsardzība vai tiesvedība, III pielikumā ir klasificētas kā augsta riska sistēmas. Līdz ar to uz tām attiecas būtiskās prasības (riska pārvaldība, testēšana, datu pārvalde, tehniskā dokumentācija, pārredzamība, cilvēka virsvadība, precizitāte, noturība un kiberdrošība) un pienākumi (piemēram, kvalitātes pārvaldības sistēmas, tehniskā dokumentācija, atbilstības novērtēšana, korektīvie pasākumi, pienākums informēt, importētāju un izplatītāju pienākumi), kā arī standarti un atbilstības novērtēšana. Šo saskaņoto noteikumu pamatā ir Direktīvā 2006/42/EK (mašīnas) ³ un Regulā (ES) 2017/745 (medicīniskas ierīces) ⁴ paredzētie noteikumi, kas attiecas uz izstrādājumu drošumu.
5. *AI* sistēmas, kas ietver reāllaika biometriskās tālidentifikācijas sistēmu izmantošanu sabiedriskās vietās tiesībaizsardzības nolūkos, ietilpst aizliegto *AI* sistēmu kategorijā. Tomēr šīm *AI* sistēmu izmantošanas aizliegumam ir paredzēti izņēmumi. Dalībvalstis var atļaut vai neatļaut šādu sistēmu izmantošanu. Ja tās ir atļautas, uz tām attiecas detalizēti ierobežojumi un aizsardzības pasākumi, kuru mērķis ir ierobežot to izmantošanu līdz apjomam, kas ir absolūti nepieciešams, un aizsargāt pamattiesības uz persondatu aizsardzību. Minētie ierobežojumi un aizsardzības pasākumi ierosinātajā regulā ir paredzēti, pamatojoties uz Līguma par Eiropas Savienības darbību ("LESD") 16. pantu, un tie ir jāpapildina ar valstu tiesību aktiem. Ierosinātās regulas 5. panta 1. punkta d) apakšpunkts un 2., 3. un 4. punkts ir *lex specialis* attiecībā uz Direktīvu (ES) 2016/680 (Direktīva par datu aizsardzību tiesībaizsardzības jomā – "DDA"), kas tika pieņemta, pamatojoties uz LESD 16. panta 2. punktu.

³ Eiropas Parlamenta un Padomes Direktīva 2006/42/EK (2006. gada 17. maijs) par mašīnām, un ar kuru groza Direktīvu 95/16/EK (OV L 157, 9.6.2006., 24.–86. lpp.).

⁴ Eiropas Parlamenta un Padomes Regula (ES) 2017/745 (2017. gada 5. aprīlis), kas attiecas uz medicīniskām ierīcēm, ar ko groza Direktīvu 2001/83/EK, Regulu (EK) Nr. 178/2002 un Regulu (EK) Nr. 1223/2009 un atceļ Padomes Direktīvas 90/385/EEK un 93/42/EEK (OV L 117, 5.5.2017., 1.–175. lpp.).

Saskaņā ar 5. panta 1. punkta d) apakšpunktu minēto sistēmu mērķi ir tikai šādi:

- i) mērķtiecīga konkrētu noziegumos potenciāli cietušo, arī pazudušu bērnu meklēšana;
- ii) īpaša, būtiska un nenovēršama apdraudējuma fizisku personu dzīvībai vai fiziskai drošībai vai teroristu uzbrukuma nepieļaušana;
- iii) vainīgā vai aizdomās turētā atklāšana, vietas noteikšana, identifikēšana vai saukšana pie atbildības par noziedzīgu nodarījumu, kas minēts Lēmuma par Eiropas apcietināšanas orderi ⁵ 2. panta 2. punktā un par ko attiecīgajā dalībvalstī var sodīt ar brīvības atņemšanu vai piemērot ar brīvības atņemšanu saistītu drošības līdzekli, kura maksimālais ilgums ir vismaz trīs gadi, kā noteikts attiecīgās dalībvalsts tiesību aktos.

Ievērojot 5. panta 3. punktu, lai tiesībaizsardzības iestādes varētu izmantot šādas tehnoloģijas, iepriekš jāsaņem tiesas vai administratīvas iestādes atļauja. Tomēr pienācīgi pamatotā steidzamā gadījumā sistēmu var sākt lietot bez atļaujas un atļauju var pieprasīt lietošanas laikā vai pēc tās.

Ievērojot 5. panta 4. punktu, dalībvalsts var nolemt atļaut reāllaika biometriskās tālidentifikācijas sistēmas izmantot sabiedriskās vietās tiesībaizsardzības nolūkos un definēt nepieciešamos sīki izstrādātos noteikumus iepriekšējās atļaujas pieprasīšanai, izdošanai un izmantošanai, kā arī saistītos noziedzīgos nodarījumus.

- 6. Ierosinātās regulas juridiskie pamati ir LESD 16. pants (persondatu aizsardzība) un 114. pants (iekšējā tirgus darbība). Tāpēc rodas jautājums par minēto juridisko pamatu atbilstību attiecībā uz saskaņotajiem noteikumiem, kas piemērojami *AI* sistēmām, kuras sagādā vai izmanto tiesībaizsardzības un tiesu iestādes.

⁵ Padomes Pamatlēmums 2002/584/TI (2002. gada 13. jūnijs) par Eiropas apcietināšanas orderi un par nodošanas procedūrām starp dalībvalstīm (OV L 190, 18.7.2002., 1. lpp.).

7. Šajā atzinumā uzmanība vispirms pievērsta LESD 114. pantā paredzētā juridiskā pamata atbilstībai, ņemot vērā to tiesībaizsardzības iestāžu īpašo kontekstu, kas minētas vairākās ierosinātās regulas normās, proti, attiecībā uz reāllaika biometriskās tālidentifikācijas sistēmām sabiedriskās vietās un augsta riska *AI* sistēmām, kas minētas III pielikuma 6. punktā. Tāpēc tajā risināts jautājums par to, vai LESD 87. panta 2. punkts (polīcijas sadarbība) – nevis LESD 114. pants (II iedaļa) – būtu atbilstošāks juridiskais pamats, lai aptvertu *AI* sistēmu sagādāšanu un izmantošanu, ko īsteno tiesībaizsardzības iestādes. Pēc analogijas šīs piezīmes secinājumu var piemērot III pielikumā minētajām tiesu iestādēm attiecībā uz augsta riska *AI* sistēmām.
8. Šajā piezīmē aplūkota arī papildu juridiskā pamata, kas paredzēts LESD 16. pantā, atbilstība un 21. un 22. protokola piemērošana saistībā ar tiesībaizsardzības īstenotu reāllaika biometriskās tālidentifikācijas sistēmu izmantošanu sabiedriskās vietās (III iedaļa).

II. LESD 114. PANTĀ PAREDZĒTĀ JURIDISKĀ PAMATA ATBILSTĪBA

9. Kā izriet no iedibinātās judikatūras, Savienības akta juridiskais pamats nav atkarīgs no iestādes pārliecības par sasniedzamo mērķi, bet ir jānosaka, balstoties uz objektīviem kritērijiem, kurus var pārbaudīt tiesā, tostarp jo īpaši uz pasākuma mērķi un saturu. Ja pasākuma pārbaudē tiek atklāts, ka tam ir divi mērķi vai divas sastāvdaļas, un ja vienu no tiem var identificēt kā galveno vai dominējošo mērķi vai sastāvdaļu, bet otram ir tikai pakārtots raksturs, tad minētais pasākums ir jābalsta tikai uz viena juridiskā pamata, proti, tā, ko prasa galvenais vai dominējošais mērķis vai sastāvdaļa. Vienīgi tad, ja ir konstatēts, ka aktam vienlaicīgi ir vairāki mērķi, kas ir nešķirami saistīti, un neviens no tiem nav pakārtots un netiešs attiecībā uz pārējiem, šādam aktam izņēmuma kārtā var būt vairāki attiecīgi juridiskie pamati, ja vien šie juridiskie pamati neparedz procedūras, kas nav savstarpēji saderīgas. Tāpat būtu jāatzīmē, ka LESD 114. panta 1. punkta pirmajā teikumā ir skaidri noteikts, ka panta noteikumus piemēro, "*[j]a vien Līgumi neparedz ko citu*". Līdz ar to LESD 114. panta izmantošana ir pamatota tikai tad, ja nav konkrētākas normas, kas varētu būt par juridisko pamatu attiecīgā pasākuma pieņemšanai ⁶. Ja Līgumā ir konkrētāka norma, kas var būt par attiecīgā pasākuma juridisko pamatu, minētais pasākums ir jāpamato ar šādu normu ⁷.

⁶ PJD 2016. gada 17. maija atzinums, 9007/16, 6. punkts.

⁷ 2004. gada 29. aprīļa spriedums lietā C-338/01, *Komisija / Padome*, EU:C:2004:253, 60. punkts.

A. IEROSINĀTĀS REGULAS MĒRKIS

10. Ierosinātā regula saskaņo konkrēta veida programmatūras (*AI* sistēmu) laišanu tirgū, nodošanu ekspluatācijā un izmantošanu. Tas, ka publiskā sektora iestādes un privātie operatori var būt šādu *AI* sistēmu sagādātāji vai lietotāji, pats par sevi nenozīmē nesaderību ar LESD 114. pantā paredzēto juridisko pamatu ⁸.
11. Turklāt tas, ka tiesībaizsardzības iestādes vai subjekti, kas rīkojas to vārdā, var būt šādu *AI* sistēmu sagādātāji vai lietotāji, nav pietiekams iemesls, ar ko pamatot LESD 87. pantā paredzētā juridiskā pamata izmantošanu. Lai noteiktu, vai tas ir nepieciešams, ir jāanalizē ierosinātās regulas mērķis un saturs.
12. Ierosinātās regulas mērķis kopumā ir nodrošināt, tostarp attiecībā uz reāllaika biometriskās tālidentifikācijas sistēmām sabiedriskās vietās un augsta riska *AI* sistēmām, konsekvētu un augstu aizsardzības līmeni visā Savienībā, vienlaikus novēršot atšķirības, kas kavē *AI* sistēmu un saistīto produktu un pakalpojumu brīvu apriti iekšējā tirgū. Tajā ir noteikti vienoti pienākumi operatoriem un garantēta sevišķi svarīgu vispārības interešu un personu tiesību vienota aizsardzība visā iekšējā tirgū (2. apsvērums). Konkrētāk, ierosinātajā regulā ir paredzēti noteikumi par konkrētu *AI* sistēmu laišanu tirgū un nodošanu ekspluatācijā, tādējādi nodrošinot netraucētu iekšējā tirgus darbību un ļaujot saistībā ar minētajām sistēmām izmantot preču un pakalpojumu brīvas pārvietošanās principa radītos ieguvumus (5. apsvērums). Kopumā priekšlikuma mērķis ir izveidot uzticamu un integrētu mākslīgo intelektu ar visaptverošu piemērojamību un pilnīgu noteikumu kopumu uz mākslīgo intelektu balstītu produktu, pakalpojumu un sistēmu izstrādei, tirdzniecībai un izmantošanai. Ņemot vērā to, ka mākslīgais intelekts jau tiek izmantots ļoti daudzos pakalpojumos un produktos un to turpinās izmantot arī turpmāk, priekšlikumā ir ievērota iekšējā tirgus loģika, definējot "produktu drošības sistēmu", kas veidota, pamatojoties uz četrām riska kategorijām. Tajā nosaka prasības ienākšanai tirgū un augsta riska *AI* sistēmu sertifikācijai, izmantojot obligātu procedūru marķēšanai ar *CE* zīmi.

⁸ Sk. PJD juridisko atzinumu (ST 11395/14, 39. līdz 41. punkts) un precedentus, piemēram, Direktīvas (ES) 2016/2102, 2014/24/ES, 2014/25/ES un 2014/23/ES.

13. Neviens no ierosinātajā regulā izvirzītajiem mērķiem neattiecas uz sabiedriskās drošības mērķu nodrošināšanu. Pat ja sabiedriskās drošības mērķus paredzēts sasniegt netieši, saskaņojot *AI* sistēmu laišanu tirgū / nodošanu ekspluatācijā / izmantošanu, ko īsteno tiesībaizsardzības iestādes, Tiesa ⁹, interpretējot LESD 87. panta 2. punktu saistībā ar LESD 67. pantu, norādīja – lai Savienības aktu, ņemot vērā tā mērķi un saturu, varētu balstīt uz LESD 87. panta 2. punktu, tam ir jābūt tieši saistītam ar LESD 67. pantā noteiktajiem mērķiem (proti, šajā gadījumā – noziedzības novēršana un policijas sadarbība). Ierosinātās regulas kontekstā tas ir izslēgts, jo vienīgie saskaņotie noteikumi par to, kā tiesībaizsardzības iestādes izmanto šādas sistēmas, ir vai nu 1) produktu drošības noteikumi, ko vienveidīgi piemēro visiem sagādātājiem un lietotājiem saistībā ar *AI* sistēmu laišanu tirgū / nodošanu ekspluatācijā vai izmantošanu, vai 2) noteikumi par persondatu aizsardzību, attiecībā uz kuriem tika pievienots LESD 16. pantā paredzētais juridiskais pamats (sk. turpmāk – III daļu).
14. Kādā citā lietā ¹⁰, lai gan Šaujamieroču direktīvas grozījuma mērķis bija nodrošināt augstāku sabiedriskās drošības līmeni saistībā ar terorisma draudiem un citiem noziedzības veidiem, Tiesa nosprieda, ka preču drošības aspektu saskaņošana ir viens no iekšējā tirgus pareizas darbības būtiskajiem elementiem, jo atšķirīgi noteikumi šajā jomā var radīt šķēršļus tirdzniecībai ¹¹.

⁹ 2014. gada 16. februāra spriedums lietā C-43/12, *Eiropas Komisija / Eiropas Parlaments un Eiropas Savienības Padome*, EU:C:2014:298.

¹⁰ 2019. gada 3. decembra spriedums lietā C-482/17, *Čehijas Republika / Eiropas Parlaments*, EU:C:2019:1035.

¹¹ Turpat, 57. punkts: "*Tā kā, pretēji Polijas Republikas apgalvotajam, šaujamieroču īpatnība ir to bīstamība ne vien to izmantotājiem, bet arī sabiedrībai, kā Tiesa ir jau norādījusi 2018. gada 23. janvāra sprieduma Buhagiar u.c. (C- 267/16, EU:C:2018:26) 54. punktā, sabiedriskās drošības apsvērumi, kā atgādināts Direktīvas 91/477 piektajā apsvērumā, šķiet nenovēršami tiesiskajā regulējumā par šo preču iegādi un glabāšanu*". Sk. arī 2018. gada 23. janvāra sprieduma lietā C-267/16, *Albert Buhagiar u.c. / Minister for Justice*, EU:C:2018:26, 54. punktu: "*Šajā ziņā ir jānorāda, ka, ņemot vērā šaujamieroču radīto risku personu drošībai, to brīva aprīte varēja tikt panākta vienīgi, paredzot stingrus nosacījumus to pārvietošanai starp dalībvalstīm, tostarp principu par iepriekšēju atļauju, kuru izsniedz dalībvalstis, kurās šādu preču pārvietošana notiek*".

15. Ierosinātās regulas mērķi, tostarp 5. panta 1. punkta d) apakšpunkts un 2., 3. un 4. punkts par reāllaika biometriskās tālidentifikācijas sistēmu izmantošana sabiedriskās vietās tiesībaizsardzības nolūkos un noteikumi par augsta riska *AI* sistēmām, kas minētas III pielikuma 6. punktā, nav tieši saistīti ar sabiedriskās drošības mērķi. Priekšlikumā drīzāk uzmanība pievērsta galvenajām bažām, kas saistītas ar to, kā *AI* sistēmas ietekmē veselību, drošību un pamattiesības. Tāpēc attiecīgās normas ir tieši saistītas ar mērķi nodrošināt vienlīdzīgus konkurences apstākļus *AI* sistēmu laišanai tirgū / nodošanai ekspluatācijā vai izmantošanai iekšējā tirgū, vienlaikus aizsargājot lietotāju veselību, drošību un pamattiesības.
16. Ņemot vērā iepriekš minēto, ierosinātās regulas galvenais mērķis ir uzlabot iekšējā tirgus darbību LESD 114. panta nozīmē, savukārt LESD 67. pantā minētie mērķi ir tikai netieši un pakārtoti saistīti ar minēto galveno mērķi.

B. IEROSINĀTĀS REGULAS SATURS

17. Ierosinātajā regulā būtībā ir ietverti noteikumi par to, kas ir nepieciešams konkrēta produkta (*AI* programmatūras) laišanai tirgū (vai tā nodošanai ekspluatācijā), ar mērķi nodrošināt, ka tas būtu drošs un tiktu ievērotas pamattiesības. Tajā ir izklāstīts pilnīgs noteikumu kopums uz mākslīgo intelektu balstītu produktu, pakalpojumu un sistēmu izstrādei, tirdzniecībai un izmantošanai. Ierosinātajā regulā nav nedz uzlikts pienākums tiesībaizsardzības iestādēm izmantot *AI* sistēmu, kura ir likumīgi laista tirgū, nedz arī tajā ir tieši reglamentēts, kā tiesībaizsardzības iestādēm būtu jāizmanto šāda *AI* sistēma. Tā vietā ir skaidri noteiktas situācijas, kad paredzētā izmantošana tiek uzskatīta par augsta riska izmantošanu tikai tāpēc, ka *AI* sistēmu izmantos tiesībaizsardzības vai tiesu iestādes.

18. Turklāt ierosinātās regulas 29. pantā ir ietverti noteikumi par augsta riska *AI* sistēmu izmantošanas nosacījumiem, taču šāda norma neattiecas uz konkrētu nozari, tai ir ierobežots tvērums (kas galvenokārt aptver produkta lietošanas instrukciju) un tā ir nesaraunami saistīta ar pienākumiem, kas saskaņā ar ierosināto regulu uzlikti *AI* sistēmu izstrādātājiem. Tā arī dod dalībvalstīm zināmu rīcības brīvību paredzēt vēl citus noteikumus par šādu augsta riska *AI* sistēmu izmantošanu. Attiecībā uz reāllaika biometriskās tālidentifikācijas sistēmu izmantošanu sabiedriskās vietās tiesībaizsardzības nolūkos (5. pants) ierosinātā regula daļēji reglamentē šādu sistēmu izmantošanu no datu aizsardzības viedokļa, pamatojoties uz LESD 16. pantu (sk. turpmāk – III daļu).
19. Turklāt tikai dalībvalstis var nolemt paredzēt iespēju pilnībā vai daļēji atļaut izmantot šādas reāllaika biometriskās tālidentifikācijas sistēmas. Konkrētie šādas izmantošanas nosacījumi joprojām ir jānosaka valsts tiesību aktos, bet tiem ir jāatbilst vispārējiem kritērijiem un aizsardzības pasākumiem, kas izklāstīti regulā: iepriekšēja tiesas vai administratīvas iestādes izsniegta atļauja, iepriekšējās atļaujas pieprasīšana, izdošana un izmantošana, kā arī to noziedzīgo nodarījumu norādīšana, saistībā ar kuriem šādu sistēmu var izmantot.

20. *AI* sistēmas ir īpašs programmatūras veids. Tādējādi saskaņotie noteikumi, ko piemēro *AI* sistēmu laišanai tirgū vai nodošanai ekspluatācijā / izmantošanai, ir produktu drošības noteikumiem līdzīgi saskaņoti noteikumi. Tos piemēro vienveidīgi, nenošķirot publiskā un privātā sektora lietotājus. Tāpēc saskaņā ar ierosinātās regulas attiecīgajiem apsvērumiem visā Savienībā būtu jānodrošina konsekvents un augsts aizsardzības līmenis. Vienlaikus būtu jānovērš atšķirības, kas kavē *AI* sistēmu un ar tām saistīto produktu un pakalpojumu brīvu apriti iekšējā tirgū. Tas tiktu sasniegts, nosakot vienotus pienākumus operatoriem un garantējot sevišķi svarīgu vispārības interešu un personu tiesību vienotu aizsardzību visā iekšējā tirgū, pamatojoties uz LESD 114. pantu ¹².
21. Ierosinātās regulas III pielikumā par augsta riska *AI* sistēmām ir vairākas atsauces uz tiesībaizsardzību, robežkontroles pārvaldību un tiesvedību (attiecīgi 6., 7. un 8. punkts). Papildus citām augsta riska sistēmām saistībā ar 6. panta 1. punktā minētajiem produktu drošības riskiem tās ietver detalizētu un izsmeļošu uzskaitījumu atbilstoši 6. panta 2. punktam. Saskaņā ar 6. panta 1. punktu dažas *AI* sistēmas ir uzskatāmas par augsta riska sistēmām pēc definīcijas, ņemot vērā to paredzamo ietekmes smagumu un augsto kaitējuma risku pamattiesībām, veselībai un drošībai. Citas sistēmas, ko uzskata par augsta riska sistēmām un kas uzskaitītas III pielikumā, ietver izglītību, kritisko infrastruktūru pārvaldību, nodarbinātību, biometrisko identifikāciju un kategorizēšanu, kā arī piekļuvi sabiedriskajiem pamatpakalpojumiem un privātiem pamatpakalpojumiem.

¹² Tāpēc ir nepieciešams Savienības tiesiskais regulējums, kas nosaka saskaņotus noteikumus mākslīgā intelekta jomā ar mērķi veicināt mākslīgā intelekta izstrādi, ieviešanu un izmantošanu iekšējā tirgū, vienlaikus nodrošinot augstu aizsardzības līmeni tādām vispārības interesēm kā veselība un drošība, un pamattiesību aizsardzība, kā tas atzīts un aizsargāts Savienības tiesību aktos. Lai sasniegtu minēto mērķi, būtu jānosaka noteikumi par konkrētu *AI* sistēmu laišanu tirgū un nodošanu ekspluatācijā, tādējādi nodrošinot netraucētu iekšējā tirgus darbību un ļaujot saistībā ar minētajām sistēmām izmantot preču un pakalpojumu brīvas pārvietošanās principa radītos ieguvumus (sk. priekšlikuma 2. un 5. apsvērumu).

22. Tomēr šādi noteikumi par augsta riska *AI* sistēmām neparedz to, vai tiesībaizsardzības un tiesu iestādēm (vai tām, kas darbojas citās identificētajās jomās) būtu vai nebūtu jāizmanto šīs sistēmas. Ierosinātā regula tikai netieši ietekmēs to *AI* sistēmu faktisko izstrādi, kuras var izmantot tiesībaizsardzības iestādes, un pašlaik izmantotās un nākotnē izmantojamās *AI* sistēmas. Tādējādi noteikumi attiecas uz *AI* sistēmām, kuras "*paredzēts izmantot*" šādās iestādēs (sk., piemēram, 3. panta 12. punktu, 8. panta 2. punktu un III pielikumu). Kāds konkrētas *AI* sistēmas iekļaušanas augsta riska sarakstā sekas ir specifiska noteikumu kopuma piemērošana riska pārvaldībai, datu pārvaldei un tehniskajām specifikācijām. Šādu augsta riska *AI* sistēmu lietotājiem ir jāievēro lietošanas instrukcijas, jāglabā žurnāldatnes un jāveic datu aizsardzības ietekmes novērtēšana.
23. Turklāt Savienības vai valsts tiesību aktos var noteikt lietotāju pienākumus, kas nav saistīti ar lietošanas instrukcijām, neskarot lietotāja rīcības brīvību organizēt savus resursus un darbības nolūkā īstenot sagādātāja norādītos cilvēka virsvadības pasākumus (ierosinātās regulas 29. panta 2. punkts). Šie noteikumi paredz papildu pamattiesību aizsardzības pasākumus augsta riska *AI* sistēmām.

24. Ņemot vērā iepriekš minēto, būtu jāuzsver, ka ierosinātajā regulā nav noteikumu, kuru mērķis būtu atļaut vai novērst to, ka tiesībaizsardzības iestādes izmanto tirgū laistu augsta riska *AI* sistēmu. Saskaņā ar ierosinātajiem noteikumiem *AI* sistēmai, ko tās paredzētās izmantošanas rezultātā izstrādā vai izmanto tiesībaizsardzības iestādes, tiks piemērots atsevišķs marķējums (augsts risks). Šādu izmantošanu reglamentētu valsts tiesību akti, un par to – zināmā mērā – lemtu pašas tiesībaizsardzības iestādes. Ierosinātās regulas 29. pantā ir noteikti (tikai attiecībā uz lietošanas instrukciju) minimālie lietošanas nosacījumi augsta riska *AI* sistēmām, tostarp tām, kas uzskaitītas III pielikuma 6., 7. un 8. punktā, un tie tiks papildināti ar valsts tiesību aktiem. Tāpēc saskaņā ar Tiesas judikatūru būtu jānošķir, no vienas puses, ierosinātās regulas iecerētais mērķis, proti, nereglamentēt *AI* sistēmu izmantošanu tiesībaizsardzības iestādēs, un, no otras puses, sekas, ko tā var netieši radīt ¹³ un kam nav nozīmes juridiskā pamata atbilstības analīzes kontekstā.
25. 6., 7. un 8. punktā uzskaitītajās jomās (attiecīgi tiesībaizsardzība, migrācija un tiesvedība) augsta riska *AI* sistēmas nav dominējošas. Saskaņā ar ierosināto regulu augsta riska *AI* sistēma ne vienmēr ir tāda, kas ir uzskaitīta III pielikumā. Lielākā daļa augsta riska sistēmu būtībā ir tās, kas vispārīgi uzskaitītas ierosinātās regulas 6. panta 1. punkta a) un b) apakšpunktā (saistībā ar produktu drošību). Citas augsta riska *AI* sistēmas ir uzskaitītas III pielikumā, aptverot 1. punktu (biometriskā identifikācija), 2. punktu (kritiskā infrastruktūra), 3. punktu (izglītība un arodmācības) un 4. punktu (nodarbinātība, darba ņēmēju pārvaldība un piekļuve pašnodarbinātībai), kuri attiecas uz jomām, kas nav saistītas ar tieslietām un iekšlietām ("TI"). Uz visiem šādu augsta riska *AI* sistēmu lietotājiem attiecas vienots režīms, kas izveidots, ņemot vērā nevis to specifisko statusu (piemēram, vai tie ir ekonomikas dalībnieki vai publiskā sektora iestādes), bet gan vērtējot no veselības, drošības un pamattiesību aizsardzības viedokļa.

¹³ Sk. Tiesas 2018. gada 21. jūnija sprieduma lietā C-5/16, *Polijas Republika / Eiropas Parlaments, Eiropas Savienības Padome*, EU:C:2018:483, 63.–68. punktu un Tiesas 2022. gada 22. jūnija sprieduma lietā C-534/20, *Leistritz AG / LH*, EU:C:2022:495, 28. punktu.

26. Tādējādi ierosinātajā regulā ir ietverti saskaņoti noteikumi par *AI* sistēmu laišanu tirgū, nodošanu ekspluatācijā un izmantošanu neatkarīgi no tā, vai tās izmanto privāti operatori vai publiskā sektora iestādes, tostarp arī ¹⁴ tiesībaizsardzības un tiesu iestādes.
27. Neskarot reāllaika biometriskās tālidentifikācijas sistēmu izmantošanu sabiedriskās vietās tiesībaizsardzības nolūkos, uz ko attiecas specifiski noteikumi par persondatu apstrādi (sk. turpmāk – III daļu), ierosinātajā regulā nav ietverti saskaņoti noteikumi par augsta riska *AI* sistēmu izmantošanu. Kā paskaidrots iepriekš 18. un 19. punktā, atsauce uz augsta riska *AI* sistēmu izmantošanu būtībā attiecas uz produkta lietošanas instrukcijām (29. pants) un ir saistīta ar izstrādātājiem uzliktajiem pienākumiem. Kā norādīts 22. punktā, lēmumu par to, vai tiesībaizsardzības vai tiesu iestādes var vai nevar izmantot augsta riska *AI* sistēmu, kas ir likumīgi laista tirgū saskaņā ar ierosināto regulu, pieņem valstu iestādes atbilstoši valsts tiesību aktiem.
28. Tāpēc LESD 87. panta 2. punkts, jo īpaši tā a) apakšpunkts, nav atbilstošs juridiskais pamats ierosinātajai regulai. Priekšlikuma noteikumi nedz veicina, nedz arī kavē attiecīgās informācijas vākšanu, glabāšanu, apstrādi, analīzi un apmaiņu. Vienkārši tad, ja šādas darbības veic tiesībaizsardzības iestādes, būs jāievēro vairāki nespecifiski, saskaņoti nosacījumi nolūkā aizsargāt lietotāju tiesības. Tāpat ierosinātās regulas izvirzītie mērķi neietver kopēju izmeklēšanas tehniku izstrādi. Ierosinātās prasības attiecībā uz augsta riska *AI* sistēmu izmantošanu nav specifiskas TI jomai un neattiecas uz policijas sadarbību šaurākā nozīmē (*stricto sensu*), kā definēts LESD.

¹⁴ Sk. Tiesas atzinuma par *Stambulas konvenciju* lietā A-1/19, EU:C:2021:198, jo īpaši 298. un 301. punktu.

29. Attiecībā uz ierosinātās regulas 5. panta 4. punkta normām dalībvalsts joprojām var nolemt reāllaika biometriskās tālidentifikācijas sistēmas atļaut izmantot sabiedriskās vietās tiesībaizsardzības nolūkos. Ja dalībvalsts tā nolemj, tai ir pienākums paredzēt nepieciešamos sīki izstrādātos noteikumus iepriekšējas atļaujas pieprasīšanai, izdošanai un izmantošanai, kā arī izklāstīt noziedzīgos nodarījumus, saistībā ar kuriem ir atļauta izmantošana izmeklēšanas vai kriminālvajāšanas nolūkos ¹⁵. Pamatojoties uz Padomē notikušo diskusiju rezultātiem, šie ierosinātie noteikumi nenozīmētu, ka attiecīgajām valsts iestādēm tiek piešķirtas jaunas pilnvaras. Tā vietā ir ierobežota esošo vai iespējamo turpmāko mehānismu izmantošana nolūkā nodrošināt tiesību uz privātumu un persondatu aizsardzību.
30. Ņemot vērā iepriekš minēto, LESD 114. pants ir vienīgais atbilstošais juridiskais pamats saskaņotiem noteikumiem par augsta riska *AI* sistēmām, tostarp tām, ko izmanto tiesībaizsardzības un tiesu iestādes, un jebkurš TI juridiskais pamats, kas iekļauts LESD Trešās daļas V sadaļā, piemēram, LESD 87. pants, attiecībā uz minētajiem saskaņotajiem noteikumiem nav ne pamatots, ne atbilstošs.

¹⁵ Jāatzīmē, ka priekšlikuma 5. panta 4. punktam ir dažas iezīmes, kas ir līdzīgas Direktīvas 2002/58 (Direktīva par elektronisko tirdzniecību) 15. panta 1. punktā iekļautajām. Konkrēti, tajā ir paredzēta iespēja dalībvalstīm atkāpties no dažiem Savienības tiesībās noteiktajiem aizliegumiem. Ņemot vērā iedibināto judikatūru, valsts tiesību normas, kuru mērķis ir atkāpties no minētā aizlieguma, katrā ziņā ietilpst Savienības tiesību tvērumā, un tas savukārt būs iemesls Hartas piemērošanai šīm normām.

III. LESD 16. PANTA KĀ PAPILDU JURIDISKĀ PAMATA ATBILSTĪBA

31. Ierosinātajā regulā kā juridiskais pamats attiecībā uz persondatu apstrādi tiesībaizsardzības jomā ir iekļauts LESD 16. pants, un tās 25. un 26. apsvērumā ir iekļauta atsauce attiecīgi uz 21. protokola 6.a pantu un 22. protokola 2.a pantu par persondatu apstrādi noziedzības novēršanas jomā. Komisija uzskata, ka LESD 16. panta vienīgais mērķis ir tā izmantošana par juridisko pamatu tiesību normām, ar kurām – papildinoši salīdzinājumā ar Direktīvu 2016/680 ("DAT direktīva") – nosaka ierobežojumus biometrisko persondatu apstrādei. 5. panta 1. punkta c) apakšpunkts ir formulēts kā principiāls aizliegums, uz kuru attiecas trīs izņēmumi. Konkrēti, reāllaika biometriskās tālidentifikācijas sistēmu izmantošana sabiedriskās vietās tiesībaizsardzības nolūkos ir aizliegta, ja vien tas nav noteikti nepieciešams, lai a) mērķtiecīgi meklētu noziegumos potenciāli cietušos, b) nepieļautu tieši draudošu teroristu uzbrukumu vai uzbrukumu personas fiziskajai neaizskaramībai / dzīvībai, c) noteiktu vainīgā vai par smagu noziegumu (ar atsauci uz Eiropas apcietināšanas orderi) aizdomās turētā atrašanās vietu vai identificētu šo personu, vai sauktu to pie atbildības. Šai specifiskajai *AI* sistēmu izmantošanu, ko veic tiesībaizsardzības iestādes, 5. panta 2., 3. un 4. punktā ir paredzētas papildu prasības, proti, nepieciešamības un samērīguma novērtējums, iepriekšēja atļauja (izņemot ārkārtas situācijas) un dalībvalstu lēmums atļaut vai neatļaut *AI* rīku specifisko izmantošanu šādās situācijās.
32. 5. pants ir sīki izstrādāta tiesību norma, kas reglamentē *AI* rīku specifisku izmantošanu un kā mērķis ir ne tikai papildināt esošo Savienības tiesisko regulējumu (DAT, kas pati balstīta uz LESD 16. pantu), taču tai ir vajadzīgs arī valsts īstenošanas satvars.

33. Būtībā, 5. panta īpašo noteikumu, lai gan tas ir formulēts kā aizliegums, var raksturot kā tādu, kas paredz stingru un izņēmuma satvaru vispārējai, reāllaika uzraudzībai, ko identifikācijas nolūkos veic ar *AI* instrumentiem attiecībā uz personām atklātās vietās. Turklāt aizliegums attiecas ne tikai uz kameru vienkāršu izmantošanu ierakstīšanai, bet arī uz *AI* rīku izmantošanu cilvēka iezīmju (tādu iezīmju kā sejas, kā arī gaita, pirkstu nospiedumi, DNS, balss, taustiņsitieni un citi biometriski vai uzvedības signāli) automātiskai atpazīšanai sabiedriskās vietās. Tas nozīmē arī vienlaicīgu datu uztveršanu un personu identificēšanu, veicot analītisku salīdzināšanu / datu pārbaudi. Turklāt šis noteikums arī jāizvērtē, ņemot vērā to, ka var tikt atļauta arī privātu lietotāju veikta identifikācija reāllaikā sabiedriskās vietās (tādiem pasākumiem kā futbola spēles).
34. Komisijas piedāvātie papildu skaidrojumi, šķiet, liecina, ka pašlaik neviena vai, iespējams, tikai pavisam nedaudzas dalībvalstis ir reglamentējušas šo konkrēto jautājumu, proti, kad tiesībaizsardzības iestādēm tiktu ļauts izmantot *AI* rīkus nolūkā reāllaikā atklātu personas sabiedriskās vietās. Tomēr praksē, lai gan nav sniegti pārliecinoši pierādījumi, kas liecinātu, ka esošā prakse un rīki būs jāmaina, šķiet skaidrs, ka turpmākajās izmeklēšanas tehnikās, kriminālistikas metodēs un noteikumos par pierādījumu vākšanu būs jāiekļauj šī aizlieguma / izņēmumu pieeja.
35. Ciktāl runa ir par juridisko pamatu, šķiet, ka normu, ar ko nosaka ierobežojumus biometrisku persondatu apstrādei papildinošā veidā (salīdzinājumā ar DAT direktīvu), mērķis ir aizsargāt persondatus, nosakot atbilstošus aizsardzības pasākumus. Šāds mērķis ir nesaraujami saistīts ar to normu mērķi, uz kurām attiecas LESD 114. pants, un neviens no tiem nav sekundārs un netiešs attiecībā pret otru. Ierosinātās regulas mērķis ir izveidot vispārēju satvaru *AI* sistēmām, izmantojot uz risku balstītu pieeju. Šajā kontekstā *AI* sistēmu horizontāla reglamentēšana var ietvert stingrus aizsardzības pasākumus, kas piemērojami šai konkrētajai *AI* sistēmai atklāšanai reāllaikā. Tāpēc šāda specifiska *AI* sistēma, kas ietver atbilstošus persondatu aizsardzības pasākumus, ir nesaraujami saistīta ar vispārējo mērķi uzlabot iekšējā tirgus darbību un nav sekundāra vai netieša attiecībā uz to. Līdz ar to saskaņā ar attiecīgo judikatūru (sk. iepriekš 9. punktu) ierosinātajai regulai vajadzēt būt duālam pamatam.

36. Tomēr paliek jautājums par to, kāds juridiskais pamats būtu jāizmanto persondatu apstrādes reglamentēšanai to sistēmu izmantošanas nolūkā, kuras minētas ierosinātās regulas 5. panta 1. punkta c) apakšpunktā līdz 4. punktā. LESD 87. panta 2. punkta a) apakšpunkts ir juridiskais pamats attiecīgas informācijas vākšanai, uzglabāšanai, apstrādei, analīzei un apmaiņai saistībā ar pasākumiem, ko tiesībaizsardzības dienesti veic noziedzīgu nodarījumu novēršanai, atklāšanai un izmeklēšanai.
37. Kā ģenerālvokāts ir paskaidrojis atzinumā par PDR nolīgumu ar Kanādu (A1/15), LESD 16. pants, no vienas puses, un LESD 87. panta 2. punkta a) apakšpunkts un 82. panta 1. punkta d) apakšpunkts, no otras puses, tomēr nevar saglabāt hierarhiska veida ("*lex generalis* – *lex specialis*") attiecības ¹⁶. LESD 16. panta 2. punkts ir vienīgā norma, kas piemērojama noteikumiem par personu aizsardzību attiecībā uz persondatu apstrādi, ko veic dalībvalstu tiesībaizsardzības iestādes, kad tās īsteno noziedzības novēršanas darbības. Tas vien, ka 5. pantā ir atsauce uz smagu noziegumu uzskaitījumu Pamatlēmumā par Eiropas apcietināšanas orderi, nemaina šo vērtējumu – minētā atsauce nenozīmē, ka ir piemērojams Pamatlēmums kā tāds ¹⁷. Smagu noziegumu uzskaitīšana ir tikai likumdevēja izmantota tehnika, lai nav jāveido atsevišķs pielikums.
38. Jāsecina, ka 5. pantā ietvertais noteikums nav līdzeklis, lai vēl vairāk ierobežotu minēto ar TI saistīto pasākumu piemērošanas nosacījumus, bet gan lai nodrošinātu, ka turpmāk jebkādā reāllaika biometriskās identifikācijas izmantošanā *AI* sistēmās pienācīgi tiktu ņemtas vērā bažas par pamattiesību ievērošanu un – galvenokārt – nepieciešamība nodrošināt to, ka biometriskie dati tiek vākti un apstrādāti, ievērojot tiesības uz privātumu un persondatu aizsardzību.
- Šajā ziņā regulas mērķis nav noteikt jaunu, obligātu TI jomai specifisku procedūru, tajā drīzāk ir ietverti izmēģināti un pārbaudīti procesuālie līdzekļi, ar kuriem nodrošināt pamattiesību ievērošanu.

¹⁶ Sk. ģenerālvokāta *P. Mengozzi* 2016. gada 8. septembra atzinuma par *Nolīguma projektu starp Kanādu un Eiropas Savienību*, Atzinums 1/15, EU:C:2016:656, 112.–120. punktu.

¹⁷ Par to, kā dalībvalstis īsteno šo smago noziegumu sarakstu, sk. Tiesas 2022. gada 21. jūnija sprieduma lietā C-817/19, *Human Rights League / Council of Ministers*, EU:C:2022:65, 150.–152. punktu.

39. Ja LESD 16. pants ir atbilstošs papildu juridiskais pamats, rodas jautājums par 21. protokola 6.a panta un 22. protokola un 2.a panta piemērošanu. Kā paskaidrots priekšlikuma 25. un 26. apsvērumā, tas nozīmē, ka tad, kad tiesībaizsardzības iestādes Īrijā vai Dānijā izmanto reāllaika biometriskās tālidentifikācijas sistēmas sabiedriskās vietās noziedzības novēršanai un ja Īrijai vai Dānijai nav saistoši attiecīgie noteikumi par policijas sadarbību vai tiesu iestāžu sadarbību krimināllietās, šīm minētajām dalībvalstīm nebūs saistošs arī ierosinātās regulas 5. panta 1. punkta d) apakšpunkts un 2. un 3. punkts. Tas nenozīmē, ka 5. panta 1. punkta d) apakšpunktā un 2. un 3. punktā ir ietverti noteikumi par policijas sadarbību, piemēram, noteikumi par informācijas apmaiņu starp tiesībaizsardzības iestādēm. Tas vienkārši nozīmē, ka ierosinātās regulas 5. panta 1. punkta d) apakšpunkts un 2. un 3. punkts līdzīgi Direktīvai 2016/680 ("DAT"), kas pieņemta, pamatojoties uz LESD 16. pantu un ir *lex generalis*, reglamentē biometrisko persondatu apstrādi specifiskā kontekstā, proti, reāllaika biometriskās tālidentifikācijas sistēmās sabiedriskās vietās noziedzības novēršanai, un neko vairāk. Komisijas priekšlikumā šajā ziņā ir ievērota pieeja, ko Savienības likumdevējs ir paturējis attiecībā uz DAT, un tādējādi ir apstiprināts, ka LESD 87. panta 2. punkta izmantošana šajā kontekstā nav pamatota.
40. LESD 16. panta pievienošana LESD 114. pantam šajā gadījumā ir pamatota ar to, ka 5. panta 1. punkta d) apakšpunkts un 2. un 3. punkts ir vienīgās situācijas, kad tiek reglamentēta tādas atļauju saņēmēmušas *AI* sistēmas izmantošana, kura aizskar tiesības uz persondatu aizsardzību, kas ir *lex specialis* attiecībā uz vispārējo datu aizsardzības regulējumu. Šādus *lex specialis* datu aizsardzības noteikumus, kas ietekmē minēto sensitīvo *AI* sistēmu izmantošanu, nevar uzskatīt par sekundāriem vai netiešiem saistībā ar iekšējā tirgus juridisko pamatu. Tāpēc LESD 16. panta kā juridiskā pamata pievienošana ierosinātajā regulā ir pietiekami pamatota, savukārt LESD 87. panta 2. punkta a) apakšpunkta izmantošana nav atbilstoša.

IV. SECINĀJUMS

41. Ņemot vērā minēto, PJD uzskata, ka:

- a) LESD 16. un 114. panta izmantošana par ierosinātās regulas juridiskajiem pamatiem ir pamatota un atbilstoša;
- b) LESD 87. panta 2. punkta vai jebkura cita TI juridiskā pamata izmantošana nav pamatota vai atbilstoša attiecībā uz saskaņotajiem noteikumiem, ko piemēro *AI* sistēmām, kuras var sagādāt vai izmantot tiesībaizsardzības vai tiesu iestādes.