



Briuselis, 2022 m. rugsėjo 12 d.
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

Tarpinstitucinė byla:
2021/0106(COD)

TEISĖS TARNYBOS NUOMONĖ ¹

nuo:	Teisės tarnybos
Dalykas:	Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės – SESV 114 ir 16 straipsnių, kaip teisėsaugos ir teisminės institucijoms taikomų nuostatų teisinio pagrindo, tinkamumas

I. IVADAS

1. Siūlomu reglamentu nustatomos suderintos dirbtinio intelekto sistemų (toliau – DI sistemos) pateikimo rinkai ir pradėjimo naudoti Sąjungoje taisyklės (toliau – siūlomas reglamentas)².

¹ Šiame dokumente pateikiamos teisinės rekomendacijos, kurioms taikoma 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais 4 straipsnio 2 dalyje numatyta apsauga ir kurių Europos Sąjungos Taryba neskelbia viešai. Taryba pasilieka galimybę neleistino paskelbimo atveju pasinaudoti visomis teisės aktų numatytais teisėmis.

² Dok. 8115/21.

2. 2022 m. balandžio 7 d. Telekomunikacijų ir informacinės visuomenės darbo grupės posėdyje Tarybos Teisės tarnyba pateikė paaiškinimus dėl dvejojo teisinio pagrindo (SESV 16 ir 114 straipsniai) tinkamumo siūlomam reglamentui dėl dirbtinio intelekto sistemų (DI sistemų). Paaiškinimuose patvirtina, kad SESV 16 ir 114 straipsniai yra tinkamas pasiūlymo teisinis pagrindas ir kad rėmimasis SESV 87 straipsnio 2 dalimi, o ne SESV 114 straipsniu, yra netinkamas. Darbo grupės prašymu šioje nuomonėje raštu išdėstomi ir išsamiau išplėtojami tame posėdyje Tarybos Teisės tarnybos atstovo pateikti paaiškinimai.
3. DI sistemos apibrėžtos siūlomo reglamento 3 straipsnio 1 dalyje. Apskritai tai yra tam tikros rūšies programinė įranga. Siūlomas reglamentas taikomas tiek tiekėjams, pateikiantiems DI sistemas rinkai, tiek tiekėjams, pradedantiems šias sistemas naudoti. Be to, siūlomas reglamentas taikomas ir naudotojams. Tiekėjas gali būti fizinis arba juridinis asmuo ar valdžios institucija (įstaiga), kurie kuria arba užsako sukurti DI sistemą, siekdami už atlygį arba nemokamai pateikti ją rinkai arba pradėti naudoti savo vardu ar su savo prekių ženklu. Naudotojas gali būti bet kuris fizinis ar juridinis asmuo, valdžios institucija, agentūra ar bet kuri kita jų įgaliota įstaiga, naudojanti DI sistemą.

4. Pagal 3 straipsnyje pateiktas apibrėžtis teisėsaugos ir teisminės institucijos galėtų būti laikomos DI sistemos tiekėjomis ir (arba) naudotojomis. DI sistemos, kurių numatytoji paskirtis, kaip apibrėžta tiekėjo, yra teisėsauga arba teisingumo vykdymas, pagal III priedą klasifikuojamos kaip didelės rizikos sistemos. Todėl joms taikomi esminiai reikalavimai (rizikos valdymas, bandymai, duomenų valdymas, techniniai dokumentai, skaidrumas, žmogaus vykdoma priežiūra, tikslumas, patikimumas ir kibernetinis saugumas) ir pareigos (pavyzdžiui, kokybės valdymo sistemos, techniniai dokumentai, atitikties vertinimas, taisomieji veiksmai, pareiga informuoti, importuotojų ir platintojų pareigos), taip pat standartai ir atitikties vertinimas. Šios suderintos taisyklės grindžiamos taisyklėmis, taikomomis gaminių saugai pagal Direktyvą 2006/42/EB (mašinos)³ ir Reglamentą 2017/745 (medicinos priemonės)⁴.
5. DI sistemos, kuriose teisėsaugos tikslais viešosiose erdvėse naudojamos tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos, priskiriamos draudžiamų DI sistemų kategorijai. Vis dėlto šiam draudimui naudoti DI sistemas taikomos išimtys. Iš tiesų valstybėse narėse tokių sistemų naudojimas gali būti leidžiamas arba neleidžiamas. Jei jas leidžiama naudoti, taikomi išsamūs apribojimai ir apsaugos priemonės, kad šios sistemos būtų naudojamos tik tada, kai tai tikrai būtina, ir siekiant apsaugoti pagrindinę teisę į asmens duomenų apsaugą. Minėti apribojimai ir apsaugos priemonės yra numatyti siūlomame reglamente remiantis Sutarties dėl Europos Sąjungos veikimo (toliau – SESV) 16 straipsniu ir turi būti papildyti nacionalinės teisės aktais. Siūlomo reglamento 5 straipsnio 1 dalies d punktas, 2, 3 ir 4 dalys yra Direktyvos (ES) 2016/680 (Duomenų apsaugos teisėsaugos srityje direktyvos), kuri buvo priimta remiantis SESV 16 straipsnio 2 dalimi, *lex specialis*.

³ 2006 m. gegužės 17 d. Europos Parlamento ir Tarybos direktyva 2006/42/EB dėl mašinų, iš dalies keičianti Direktyvą 95/16/EB (OL L 157, 2006 6 9, p. 24–86).

⁴ 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/745 dėl medicinos priemonių, kuriuo iš dalies keičiama Direktyva 2001/83/EB, Reglamentas (EB) Nr. 178/2002 ir Reglamentas (EB) Nr. 1223/2009, ir kuriuo panaikinamos Tarybos direktyvos 90/385/EEB ir 93/42/EEB (OL L 117, 2017 5 5, p. 1–175).

Pagal 5 straipsnio 1 dalies d punktą tos sistemos naudojamos tik siekiant šių tikslų:

- i) vykdam tikslinę konkrečių galimų nusikaltimo aukų, įskaitant dingusius vaikus, paiešką;
- ii) siekiant išvengti konkrečios didelės artėjančios grėsmės fizinių asmenų gyvybei ar fizinei saugai arba teroristinio išpuolio;
- iii) siekiant išaiškinti asmenis, padariusius Sprendimo dėl Europos arešto orderio⁵ 2 straipsnio 2 dalyje nurodytą nusikalstamą veiką, už kurią atitinkamoje valstybėje narėje jos teisėje nustatyta tvarka baudžiama laisvės atėmimo bausme arba įkalinimu, kurio ilgiausias terminas – bent treji metai, arba asmenis, įtariamus tokios veikos padarymu, nustatyti jų buvimo vietą ar tapatybę arba patraukti juos baudžiamojon atsakomybėn.

Pagal 5 straipsnio 3 dalį teisėsaugos institucijos turi gauti išankstinį teisminės arba administracinės institucijos leidimą naudoti tokias technologijas. Tačiau tinkamai pagrįstais skubos atvejais sistemą galima pradėti naudoti be leidimo, o leidimo prašyti naudojant sistemą arba baigus ją naudoti.

Pagal 5 straipsnio 4 dalį valstybė narė gali nuspręsti leisti naudoti tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemas viešosiose erdvėse teisėsaugos tikslais ir nustatyti būtinas išsamias taisykles, kuriomis reglamentuojama išankstinių leidimų prašymo, išdavimo ir vykdymo tvarka, taip pat susijusi nusikalstama veika.

6. Siūlomo reglamento teisinis pagrindas yra SESV 16 straipsnis (asmens duomenų apsauga) ir 114 straipsnis (vidaus rinkos veikimas). Todėl kyla klausimas dėl tų teisinių pagrindų tinkamumo suderintoms taisyklėms, taikomoms teisėsaugos ir teisminių institucijų tiekiamoms ar naudojamoms DI sistemoms.

⁵ 2002 m. birželio 13 d. Tarybos pagrindų sprendimas 2002/584/TVR dėl Europos arešto orderio ir perdavimo tarp valstybių narių tvarkos (OL L 190, 2002 7 18, p. 1).

7. Šioje nuomonėje daugiausia dėmesio visų pirma skiriama SESV 114 straipsnio, kaip teisinio pagrindo, tinkamumui, atsižvelgiant į konkrečias teisėsaugos institucijų, paminėtų keliose siūlomo reglamento nuostatose, t. y. dėl tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų viešosiose erdvėse ir III priedo 6 punkte nurodytų didelės rizikos DI sistemų, aplinkybes. Todėl joje nagrinėjamas klausimas, ar SESV 87 straipsnio 2 dalis (policijos bendradarbiavimas), o ne SESV 114 straipsnis (II skirsnis), būtų tinkamesnis teisinis pagrindas, kuriuo remiantis būtų galima reglamentuoti teisėsaugos institucijų vykdomą DI sistemų tiekimą ir naudojimą. Pagal analogiją šio pranešimo išvada gali būti taikoma III priede dėl didelės rizikos DI sistemų nurodytoms teisminėms institucijoms.
8. Šiame pranešime taip pat nagrinėjamas SESV 16 straipsnio, kaip papildomo teisinio pagrindo, tinkamumas ir protokolų Nr. 21 ir Nr. 22 taikymas, kai teisėsaugos institucijos naudoja tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemas viešosiose erdvėse (III skirsnis).

II. SESV 114 STRAIPSNIO, KAIP TEISINIO PAGRINDO, TINKAMUMAS

9. Pagal nusistovėjusią teismo jurisprudenciją Sąjungos akto teisinis pagrindas nepriklauso nuo institucijos įsitikinimo, susijusio su tikslu, kurio siekiama, bet turi būti nustatomas laikantis objektyvių kriterijų, kuriems gali būti taikoma teisminė peržiūra, įskaitant visų pirma priemonės tikslą ir turinį. Jeigu išnagrinėjus priemonę paaiškėja, kad ja siekiama dvejopo tikslo arba tikslas turi dvi sudedamąsias dalis, ir jei vieną iš šių tikslų arba vieną iš šių dalių galima išskirti kaip pagrindinį (-ę) ar dominuojantį (-čią), o kitą tik kaip papildomą, priemonė turi būti grindžiama tik vienu teisiniu pagrindu – tuo, kurio reikalauja pagrindinis ar dominuojantis tikslas arba pagrindinė ar dominuojanti sudedamoji dalis. Tik išimtiniais atvejais, jeigu nustatoma, kad aktu tuo pat metu siekiama kelių neatsiejamai susijusių tikslų, kurių nė vienas nėra papildomas ir netiesioginis kito atžvilgiu, toks aktas gali būti grindžiamas įvairiais atitinkamais teisiniais pagrindais, nebent tuose teisiniuose pagrinduose būtų numatytos viena su kita nesuderinamos procedūros. Taip pat reikėtų pažymėti, kad SESV 114 straipsnio 1 dalies pirmame sakinyje aiškiai nurodyta, jog to straipsnio nuostatos taikomos „[i]šskyrus tuos atvejus, kai Sutartyse nustatyta kitaip“. Taigi, rėmimasis SESV 114 straipsniu yra pateisinamas tik tuo atveju, kai nėra labiau specifinių nuostatų, kurios galėtų būti nagrinėjamos priemonės priėmimo teisinis pagrindas⁶. Jeigu Sutartyje yra labiau specifinė nuostata, tinkama būti tam tikros priemonės teisiniu pagrindu, ta priemonė turi būti pagrindžiama tokia nuostata⁷.

⁶ 2016 m. gegužės 17 d. Tarybos Teisės tarnybos nuomonės 9007/16 6 punktas.

⁷ 2004 m. balandžio 29 d. Sprendimo *Komisija / Taryba*, C- 338/01, EU:C:2004:253, 60 punktas.

A. SIŪLOMO REGLAMENTO TIKSLAS

10. Siūlomą reglamentu suderinamas tam tikros rūšies programinės įrangos (DI sistemų) pateikimas rinkai, pradėjimas naudoti ir naudojimas. Tai, kad valdžios institucijos ir privačiojo sektoriaus veiklos vykdytojai gali būti tokių DI sistemų tiekėjai ar naudotojai, savaime nėra nesuderinama su SESV 114 straipsniu, kaip teisiniu pagrindu⁸.
11. Be to, tai, kad teisėsaugos institucijos arba jų vardu veikiantys asmenys gali būti vieni iš tokių DI sistemų tiekėjų arba naudotojų, nėra pakankamas pagrindas remtis SESV 87 straipsniu, kaip teisiniu pagrindu. Siekiant nustatyti, ar tai būtina, reikia išnagrinėti siūlomo reglamento tikslą ir turinį.
12. Siūlomą reglamentu apskritai siekiama, taip pat tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų viešosiose erdvėse bei didelės rizikos DI sistemų atžvilgiu, užtikrinti nuoseklią ir aukšto lygio apsaugą visoje Sąjungoje, kartu užkertant kelią skirtumams, trukdantiems laisvam DI sistemų ir susijusių gaminių bei paslaugų judėjimui vidaus rinkoje. Jame nustatomos vienodos veiklos vykdytojų pareigos ir užtikrinama vienoda svarbių viešojo intereso priežasčių ir asmenų teisių apsauga visoje vidaus rinkoje (2 konstatuojamoji dalis). Konkrečiau, siūlomame reglamente nustatytos taisyklės, kuriomis reglamentuojamas tam tikrų DI sistemų pateikimas rinkai ir pradėjimas naudoti, taip užtikrinant sklandų vidaus rinkos veikimą ir leidžiant išnaudoti tų sistemų privalumus, atsižvelgiant į prekių ir paslaugų laisvo judėjimo principą (5 konstatuojamoji dalis). Apskritai pasiūlymu siekiama sukurti patikimą integruotąjį DI, taikomą visose srityse, ir nustatyti išsamias DI grindžiamų gaminių, paslaugų ir sistemų kūrimo, pateikimo rinkai ir naudojimo taisykles. Atsižvelgiant į tai, kad dirbtinis intelektas jau dabar naudojamas daugybėje paslaugų ir gaminių ir kad jis bus naudojamas ateityje, pasiūlyme vadovaujamasi vidaus rinkos logika nustatant „gaminių saugos sistemą“, pagrįstą keturiomis rizikos kategorijomis. Jame nustatomi didelės rizikos DI sistemų pateikimo į rinką ir sertifikavimo reikalavimai taikant privalomą ženklinimo CE ženklų procedūrą.

⁸ Žr. Teisės tarnybos teisinę nuomonę (ST 11395/14, 39–41 punktai) ir precedentes, pavyzdžiui, Direktyvą (ES) 2016/2102, direktyvas 2014/24/ES, 2014/25/ES ir 2014/23/ES.

13. Nė vienas iš nurodytų siūlomo reglamento tikslų nėra susijęs su visuomenės saugumo tikslų įgyvendinimu. Net jei visuomenės saugumo tikslai turi būti netiesiogiai pasiekti derinant teisėsaugos institucijų vykdomą DI sistemų pateikimo rinkai / pradėjimo naudoti / naudojimo procesą, Teisingumo Teismas⁹, aiškindamas SESV 87 straipsnio 2 dalį atsižvelgiant į SESV 67 straipsnį, nurodė, jog tam, kad Sąjungos aktas, atsižvelgiant į jo tikslą ir turinį, būtų grindžiamas SESV 87 straipsnio 2 dalimi, jis turi būti tiesiogiai susijęs su SESV 67 straipsnyje nustatytais tikslais (t. y. šiuo atveju – nusikaltimų prevencija ir policijos bendradarbiavimu). Taip nėra siūlomo reglamento atveju, nes vienintelės suderintos taisyklės dėl teisėsaugos institucijų naudojimosi tokiais sistemomis yra 1) su gaminių sauga susijusios taisyklės, vienodai taikomos visiems tiekėjams ir naudotojams, kiek tai susiję su DI sistemų pateikimu rinkai / pradėjimu naudoti arba naudojimu, arba 2) asmens duomenų apsaugos taisyklės, dėl kurių įtrauktas teisinis pagrindas – SESV 16 straipsnis (žr. šios nuomonės III dalį).
14. Kitoje byloje¹⁰, nors Direktyvos dėl šaunamųjų ginklų direktyvos pakeitimo tikslas buvo užtikrinti aukštesnį visuomenės saugumo nuo terorizmo grėsmės ir kitų nusikalstamumo formų lygį, Teisingumo Teismas nusprendė, kad aspektų, susijusių su prekių saugumu, suderinimas yra vienas iš esminių elementų siekiant užtikrinti tinkamą vidaus rinkos veikimą, nes šioje srityje priimti nesuderinti teisės aktai gali sukurti kliūčių prekybai¹¹.

⁹ 2014 m. gegužės 6 d. Sprendimas *Lenkija / Europos Parlamentas ir Europos Sąjungos Taryba*, C-43/12, ECLI:EU:C:2014:298.

¹⁰ 2019 m. gruodžio 3 d. Sprendimas *Čekija / Parlamentas ir Taryba*, C-482/17, EU:C:2019:1035.

¹¹ Ten pat, 57 punktas: „[k]adangi šaunamųjų ginklų ypatybė yra, priešingai, nei teigia Lenkijos Respublika, jų pavojingumas ne tik jų naudotojams, bet plačiai visuomenei, kaip Teisingumo Teismas jau nurodė 2018 m. sausio 23 d. Sprendimo *Buhagiar ir kt.* (C267/16, EU:C:2018:26) 54 punkte, į visuomenės saugumo sumetimus, kaip tai primenama ir Direktyvos 91/477 penktoje konstatuojamojoje dalyje, būtina atsižvelgti nustatant šių prekių įsigijimo ir laikymo reglamentavimą.“ Taip pat žr. 2018 m. sausio 23 d. Sprendimo *Albert Buhagiar ir kt. / Teisingumo ministras*, C-267/16, EU:C:2018:26, 54 punktą: „[š]iuo aspektu svarbu pažymėti, kad, atsižvelgiant į pavojų, kurį asmenų saugumui kelia šaunamieji ginklai, jų laisvą judėjimą galima buvo pasiekti tik nustatant griežtas jų perdavimo iš vienos valstybės narės į kitą sąlygas, tarp kurių yra valstybių narių, susijusių su tokių prekių perdavimu, išduodamo išankstinio leidimo principas.“

15. Siūlomo reglamento tikslai, įskaitant 5 straipsnio 1 dalies d punktą, 2, 3 ir 4 dalis dėl tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimo viešosiose erdvėse teisėsaugos tikslais ir III priedo 6 punkte nurodytas nuostatas, susijusias su didelės rizikos DI sistemomis, nėra tiesiogiai susiję su visuomenės saugumo tikslu. Priešingai, pasiūlymu reaguojama į pagrindinius susirūpinimą keliančius klausimus, susijusius su DI sistemų poveikiu sveikatai, saugai ir pagrindinėms teisėms. Todėl atitinkamos nuostatos yra tiesiogiai susijusios su tikslu užtikrinti vienodas sąlygas DI sistemų pateikimo rinkai / pradėjimo naudoti arba naudojimo vidaus rinkoje srityje, kartu apsaugant naudotojų sveikatą, saugą ir pagrindines teises.
16. Atsižvelgiant į tai, kas išdėstyta pirmiau, pagrindinis siūlomo reglamento tikslas – pagerinti vidaus rinkos veikimą, kaip apibrėžta SESV 114 straipsnyje, o SESV 67 straipsnyje nurodyti tikslai yra tik netiesiogiai ir atsitiktinai susiję su minėtu pagrindiniu tikslu.

B. SIŪLOMO REGLAMENTO TURINYS

17. Siūlomame reglamente iš esmės pateikiamos taisyklės dėl to, ko reikia norint pateikti rinkai (arba pradėti naudoti) konkretų gaminį (DI programinę įrangą), siekiant užtikrinti, kad jis būtų saugus ir nepažeistų pagrindinių teisių. Jame nustatytos išsamios DI grindžiamų gaminių, paslaugų ir sistemų kūrimo, pateikimo rinkai ir naudojimo taisyklės. Siūlomu reglamentu teisėsaugos institucijos neįpareigojamos naudoti teisėtu būdu rinkai pateiktos DI sistemos ir tiesiogiai nereglamentuojama, kaip teisėsaugos institucijos turėtų naudoti tokią DI sistemą. Tačiau jame aiškiai nustatomi atvejai, kai numatoma paskirtis laikoma keliančia didelę riziką vien dėl to, kad DI sistemą naudos teisėsaugos arba teisminės institucijos.

18. Beje, siūlomo reglamento 29 straipsnyje pateikiamos taisyklės dėl didelės rizikos DI sistemų naudojimo sąlygų, tačiau tokia nuostata nėra skirta konkrečiam sektoriui, jos taikymo sritis yra ribota (daugiausia apima gaminių naudojimo instrukcijas) ir ji yra iš esmės susijusi su DI sistemų kūrėjams pagal siūlomą reglamentą nustatytomis pareigomis. Reglamente valstybėms narėms taip pat suteikiama tam tikra veiksmų laisvė nustatyti papildomas tokių didelės rizikos DI sistemų naudojimo taisykles. Kalbant apie tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemas, naudojamas viešosiose erdvėse teisėsaugos tikslais (5 straipsnis), siūlomu reglamentu iš dalies reglamentuojamas tokių sistemų naudojimas duomenų apsaugos požiūriu, remiantis SESV 16 straipsniu (žr. šios nuomonės III dalį).
19. Be to, tik valstybės narės gali nuspręsti numatyti galimybę visiškai arba iš dalies leisti naudoti tokias tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemas. Konkrečios tokio naudojimo sąlygos turi būti nustatytos nacionalinėje teisėje, tačiau turi būti laikomasi reglamente nustatytų bendrųjų kriterijų ir apsaugos priemonių: išankstinis teismo ar administracinės institucijos leidimas, prašymas, išankstinio leidimo išdavimas ir vykdymas, taip pat nusikalstamų veikų, kurių atžvilgiu gali būti naudojamos tokios sistemos, nurodymas.

20. DI sistemos yra tam tikros rūšies programinė įranga. Taigi suderintos taisyklės, taikomos pateikiant rinkai arba pradėdant naudoti / naudojant DI sistemas, yra panašios į suderintas gaminių saugos taisykles. Jos taikomos vienodai, neatskiriant viešųjų ir privačiųjų naudotojų. Todėl pagal atitinkamas siūlomo reglamento konstatuojamąsias dalis visoje Sąjungoje turėtų būti užtikrinta nuosekli ir aukšto lygio apsauga. Kartu reikėtų užkirsti kelią skirtumams, trukdantiems laisvam DI sistemų ir susijusių gaminių bei paslaugų judėjimui vidaus rinkoje. Tai būtų pasiekta nustatant vienodas pareigas veiklos vykdytojams ir garantuojant vienodą svarbių viešojo intereso priežasčių ir asmenų teisių apsaugą visoje vidaus rinkoje, remiantis SESV 114 straipsniu¹².
21. Siūlomo reglamento III priede dėl didelės rizikos DI sistemų yra keletas nuorodų į teisėsaugą, sienų kontrolės valdymą ir teisingumo vykdymą (atitinkamai 6, 7 ir 8 punktai). Pateiktas išsamus ir baigtinis sąrašas pagal 6 straipsnio 2 dalį, papildantis kitas didelės rizikos sistemas, susijusias su 6 straipsnio 1 dalyje nurodyta gaminių saugos rizika. Iš tiesų pagal 6 straipsnio 1 dalį kai kurios DI sistemos iš esmės turi būti laikomos didelės rizikos sistemomis dėl numatomo jų rizikos dydžio ir didelės rizikos pagrindinėms teisėms, sveikatai ir saugai. Kitos sistemos, laikomos keliančiomis didelę riziką ir išvardytos III priede, apima švietimą, ypatingos svarbos infrastruktūros objektų valdymą, užimtumą, biometrinį tapatybės nustatymą ir kategorizavimą, taip pat galimybę gauti esmines privačiasias ir viešąsias paslaugas.

¹² Todėl Sąjungos teisinė sistema, kuria nustatomos suderintos dirbtinio intelekto taisyklės, yra reikalinga siekiant vidaus rinkoje skatinti kurti, naudoti ir įsisavinti dirbtinį intelektą, kartu užtikrinant aukšto lygio viešųjų interesų, kaip antai saugos ir sveikatos apsaugą, ir pagrindinių teisių apsaugą, pripažįstama ir saugoma Sąjungos teisėje. Kad šis tikslas būtų pasiektas, reikėtų nustatyti taisykles, kuriomis reglamentuojamas tam tikrų DI sistemų pateikimas rinkai ir pradėjimas naudoti, taip užtikrinant sklandų vidaus rinkos veikimą ir leidžiant išnaudoti tų sistemų privalumus, atsižvelgiant į prekių ir paslaugų laisvo judėjimo principą (žr. pasiūlymo 2 ir 5 konstatuojamąsias dalis).

22. Tačiau tokiose didelės rizikos DI sistemų taisyklėse nenumatyta, ar teisėsaugos ir teisminės institucijos (arba kitose nustatytose srityse veikiančios institucijos) turėtų naudoti tas sistemas, ar ne. Siūlomas reglamentas turės tik netiesioginį poveikį faktiniam DI sistemų, kurias gali naudoti teisėsaugos institucijos, kūrimui ir dabar naudojamoms bei ateities DI sistemoms. Taigi taisyklėse nurodomos DI sistemos, kurias „*numatoma naudoti*“ tokiose institucijose (žr., pvz., 3 straipsnio 12 dalį, 8 straipsnio 2 dalį ir III priedą). Tam tikrą DI sistemą įtraukus į didelės rizikos DI sistemų sąrašą, taikomos konkrečios taisyklės dėl rizikos valdymo, duomenų valdymo ir techninių specifikacijų. Tokių didelės rizikos DI sistemų naudotojai turi laikytis naudojimo instrukcijų, registruoti duomenis ir atlikti poveikio duomenų apsaugai vertinimus.
23. Be to, naudotojo pareigos, nesusijusios su naudojimo instrukcijomis, gali būti nustatytos Sąjungos arba nacionalinėje teisėje, nedarant poveikio naudotojų laisvei savo nuožiūra organizuoti savo išteklius ir veiklą siekiant taikyti tiekėjo nurodytas žmogaus vykdomos priežiūros priemonės (siūlomo reglamento 29 straipsnio 2 dalis). Šiomis taisyklėmis numatomos papildomos pagrindinių teisių apsaugos priemonės, taikomos didelės rizikos DI sistemoms.

24. Atsižvelgiant į tai, kas išdėstyta pirmiau, reikėtų pabrėžti, kad siūlomame reglamente nėra taisyklių, kuriomis būtų siekiama leisti arba neleisti teisėsaugos institucijoms naudoti rinkai pateiktą didelės rizikos DI sistemą. Remiantis siūlomomis taisyklėmis, DI sistemai, sukurtai arba naudojamai teisėsaugos institucijų pagal numatomą paskirtį, bus taikomas atskiras ženklinimas (didelės rizikos). Šis naudojimas būtų reglamentuojamas pagal nacionalinę teisę, tam tikru mastu dėl jo spęstų pačios teisėsaugos institucijos. Iš tiesų siūlomo reglamento 29 straipsnyje nustatomos didelės rizikos DI sistemų, įskaitant išvardytąsias III priedo 6, 7 ir 8 punktuose, būtiniausios naudojimo sąlygos (tik naudojimo instrukcijos), kurios bus papildytos nacionalinės teisės aktais. Todėl, remiantis Teismo jurisprudencija, reikėtų atskirti numatytą siūlomo reglamento tikslą, kuriuo nesiekama reguliuoti teisėsaugos institucijų naudojimosi DI sistemomis, nuo galimo jo netiesioginio poveikio¹³, kuris nėra svarbus analizuojant teisinio pagrindo tinkamumą.
25. 6, 7 ir 8 punktuose (atitinkamai dėl teisėsaugos, migracijos ir teisingumo vykdymo) nurodytos sistemos nėra dominuojančios tarp didelės rizikos DI sistemų. Iš tiesų pagal siūlomą reglamentą didelės rizikos DI sistema nebūtinai yra III priede nurodyta sistema. Dauguma didelės rizikos sistemų iš tiesų yra siūlomo reglamento 6 straipsnio 1 dalies a ir b punktuose bendrai išvardytos sistemos (susijusios su gaminių sauga). Kitos didelės rizikos DI sistemos yra išvardytos III priedo 1 punkte (biometrinis identifikavimas), 2 punkte (ypatingos svarbos infrastruktūra), 3 punkte (švietimas ir profesinis mokymas) ir 4 punkte (užimtumas, darbuotojų valdymas ir galimybė dirbti savarankiškai), kurie susiję su kitomis sritimis nei teisingumas ir vidaus reikalai (toliau – TVR). Visiems tokių didelės rizikos DI sistemų naudotojams taikoma vienoda tvarka, nustatyta ne pagal jų konkretų statusą (pvz., ekonominės veiklos vykdytojai ar valdžios institucijos), bet atsižvelgiant į sveikatos, saugos ir pagrindinių teisių apsaugą.

¹³ Žr. 2018 m. birželio 21 d. Sprendimo *Lenkijos Respublika / Europos Parlamentas, Europos Sąjungos Taryba*, C-5/16, EU:C:2018:483, 63–68 punktus ir 2022 m. birželio 22 d. Sprendimo *Leistritz AG / LH*, C-534/20, EU:C:2022:495, 28 punktą.

26. Todėl siūlomame reglamente pateikiamos suderintos taisyklės dėl DI sistemų pateikimo rinkai, pradėjimo naudoti ir naudojimo, neatsižvelgiant į tai, ar jas naudoja privačiojo sektoriaus veiklos vykdytojai ar valdžios institucijos, įskaitant, beje¹⁴, teisėsaugos ir teismines institucijas.
27. Be tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimo viešosiose erdvėse teisėsaugos tikslais, kuriam taikomos konkrečios asmens duomenų tvarkymo taisyklės (žr. šios nuomonės III dalį), siūlomame reglamente nėra suderintų didelės rizikos DI sistemų naudojimo taisyklių. Kaip paaiškinta šios nuomonės 18 ir 19 punktuose, nuoroda į didelės rizikos DI sistemų naudojimą iš esmės susijusi su gaminių naudojimo instrukcijomis (29 straipsnis) ir su kūrėjams nustatytomis pareigomis. Kaip nurodyta 22 punkte, sprendimą dėl to, ar teisėsaugos arba teisminės institucijos gali naudoti didelės rizikos DI sistemą, teisėtai pateiktą rinkai pagal siūlomą reglamentą, priima nacionalinės institucijos pagal nacionalinę teisę.
28. Todėl SESV 87 straipsnio 2 dalis, ypač jos a punktas, nėra tinkamas siūlomo reglamento teisinis pagrindas. Pasiūlyme išdėstytomis taisyklėmis nei skatinama, nei trukdoma rinkti, saugoti, apdoroti, analizuoti svarbią informaciją ar ją keistis. Tiesiog, kai tokią veiklą vykdo teisėsaugos institucijos, jos turi laikytis keleto nekonkrečių, suderintų sąlygų, kad būtų apsaugotos naudotojų teisės. Be to, nurodyti siūlomo reglamento tikslai neapima bendrų tyrimo metodų parengimo. Siūlomi didelės rizikos DI sistemų naudojimo reikalavimai nėra konkrečiai skirti TVR sričiai ir nėra susiję su policijos bendradarbiavimu *stricto sensu*, kaip apibrėžta SESV.

¹⁴ Žr. Teisingumo Teismo išvadą dėl *Stambulo konvencijos*, A-1/19, EU:C:2021:198, ypač 298 ir 301 punktus.

29. Atsižvelgdama į siūlomo reglamento 5 straipsnio 4 dalies nuostatas, valstybė narė vis tiek gali nuspręsti leisti naudoti tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemas viešosiose erdvėse teisėsaugos tikslais. Taip nusprendusi, valstybė narė privalo nustatyti būtinas išsamias prašymo išduoti išankstinį leidimą, išankstinio leidimo išdavimo ir jo vykdymo taisykles, taip pat susijusias nusikalstamas veikas, kurių tyrimui ar baudžiamajam persekiojimui sistemas leidžiama naudoti¹⁵. Remiantis diskusijų Taryboje rezultatais, dėl šių siūlomų taisyklių atitinkamoms nacionalinėms valdžios institucijoms nebūtų suteikti nauji įgaliojimai. Tačiau, siekiant užtikrinti teisės į privatumą ir asmens duomenų apsaugą, ribojamas esamų ar galimų būsimų mechanizmų naudojimas.
30. Atsižvelgiant į tai, kas išdėstyta pirmiau, SESV 114 straipsnis yra vienintelis tinkamas suderintų taisyklių dėl didelės rizikos DI sistemų, įskaitant teisėsaugos ir teisminių institucijų naudojamas DI sistemas, teisinis pagrindas, o bet koks SESV trečiosios dalies V antraštinėje dalyje nustatytas su TVR susijęs teisinis pagrindas, pavyzdžiui, SESV 87 straipsnis, tų suderintų taisyklių atžvilgiu nėra nei pagrįstas, nei tinkamas.

¹⁵ Pažymėtina, kad pasiūlymo 5 straipsnio 4 dalis tam tikrais aspektais panaši į E. privatumo direktyvos 2002/58 15 straipsnio 1 dalį. Visų pirma joje numatyta galimybė valstybėms narėms nukrypti nuo tam tikrų Sąjungos teisėje nustatytų draudimų. Atsižvelgiant į suformuotą jurisprudenciją, nacionalinės teisės nuostatos, kuriomis siekiama nukrypti nuo minėtų draudimų, tikrai patenka į Sąjungos teisės taikymo sritį, o tai savo ruožtu lemia Chartijos taikymą jų atžvilgiu.

III. SESV 16 STRAIPSNIO, KAIP PAPILDOMO TEISINIO PAGRINDO, TINKAMUMAS

31. Siūlomame reglamente kaip teisinis pagrindas nurodytas ir SESV 16 straipsnis, susijęs su asmens duomenų tvarkymu teisėsaugos srityje; jo 25 ir 26 konstatuojamosiose dalyse pateikta nuoroda į Protokolo Nr. 21 6a straipsnį ir Protokolo Nr. 22 dėl asmens duomenų tvarkymo nusikaltimų prevencijos srityje 2a straipsnį. Komisijos nuomone, SESV 16 straipsniu siekiama sukurti teisinį pagrindą tik nuostatoms, kuriomis papildomi biometrinių asmens duomenų tvarkymo apribojimai, palyginti su Direktyva (ES) 2016/680 (Duomenų apsaugos teisėsaugos srityje direktyvoje). 5 straipsnio 1 dalies d punktas suformuluotas kaip principinis draudimas, kuriam taikomos trys išimtys. Konkrečiai, tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimas viešosiose erdvėse teisėsaugos tikslais yra draudžiamas, išskyrus atvejus, kai tai tikrai būtina siekiant: a) vykdyti tikslinę galimų nusikaltimų aukų paiešką; b) užkirsti kelią gresiančiam teroristų išpuoliui arba išpuoliui prieš asmens fizinę neliečiamybę / gyvybę; c) nustatyti sunkų nusikaltimą padariusio asmens arba įtariamojo buvimo vietą arba jo tapatybę arba patraukti jį baudžiamojon atsakomybėn (remiantis Europos arešto orderiu). Šiam konkrečiam DI sistemų naudojimui teisėsaugos institucijose taikytini papildomi 5 straipsnio 2, 3 ir 4 dalyse nustatyti reikalavimai, visų pirma dėl būtinumo ir proporcingumo vertinimo, išankstinio leidimo (išskyrus ekstremalios padėties atvejų) ir valstybių narių sprendimo, ar nacionaliniu lygmeniu leisti tikslinę DI priemonių naudojimą tokiais atvejais.
32. 5 straipsnis yra išsami nuostata, reglamentuojanti konkretų DI priemonių naudojimą, kuria siekiama papildyti esamą Sąjungos teisės aktų sistemą (Duomenų apsaugos teisėsaugos srityje direktyvą, pagrįstą SESV 16 straipsniu), tačiau jai reikalinga ir nacionalinė įgyvendinimo sistema.

33. Iš esmės, nepaisant to, kad 5 straipsnyje nustatyta konkreti taisyklė suformuluota kaip draudimas, ji gali būti apibūdinta kaip nustatanti griežtą ir išimtinę DI priemonėmis vykdomo atvirose erdvėse esančių asmenų bendro, tikralaikio stebėjimo, siekiant nustatyti jų tapatybę, sistemą. Be to, draudimas neapsiriboja įprastiniu filmavimo kamerų naudojimu įrašymui, bet apima DI priemonių naudojimą automatizuotam žmogaus savybių (tokių kaip veidas, taip pat eisena, pirštų atspaudai, DNR, balsas, klavišų paspaudimai ir kiti biometriniai ar elgsenos požymiai) atpažinimui viešosiose erdvėse. Tai taip pat reiškia, kad tuo pačiu metu asmenys fiksuojami ir identifikuojami, atliekant duomenų analizę, palyginimą / patikrinimą. Be to, ši taisyklė taip pat turi būti vertinama atsižvelgiant į tai, kad privatiems naudotojams gali būti leidžiamas tikralaikis tapatybės nustatymas viešosiose erdvėse (pvz., tokiuose renginiuose kaip futbolo rungtynės).
34. Iš papildomų Komisijos pateiktų paaiškinimų matyti, kad šiuo metu šio konkretaus klausimo nereglamentuoja nė viena valstybė narė arba reglamentuoja vos kelios, kad teisėsaugos institucijos galėtų naudoti DI priemones tikralaikiam asmenų aptikimui viešosiose erdvėse. Tačiau praktiškai, nors nebuvo pateikta patikimų įrodymų, kad esamą praktiką ir priemones reikės keisti, atrodo aišku, kad į būsimus tyrimo metodus, teismo ekspertizės metodus ir įrodymų rinkimo taisykles turės būti įtrauktas ir šis draudimų / išimčių metodas.
35. Kalbant apie teisinį pagrindą, atrodo, kad nuostatomis, kuriomis papildomi biometrinių asmens duomenų tvarkymo apribojimai (palyginti su Duomenų apsaugos teisėsaugos srityje direktyva), siekiama apsaugoti asmens duomenis nustatant tinkamas apsaugos priemones. Toks tikslas neatsiejamai susijęs su nuostatų, patenkančių į SESV 114 straipsnio taikymo sritį, tikslu ir nė vienas iš jų nėra papildomas ir netiesioginis kito atžvilgiu. Siūlomam reglamentui siekiama nustatyti bendrą DI sistemų pagrindą, laikantis rizika grindžiamo požiūrio. Atsižvelgiant į tai, horizontaliai reguliuojant DI sistemas gali būti numatytos griežtos apsaugos priemonės, taikytinos šiai konkrečiai tikralaikio aptikimo DI sistemai. Todėl tokia konkreti DI sistema, kurioje numatytos tinkamos asmens duomenų apsaugos priemonės, yra neatsiejama nuo bendro tikslo pagerinti vidaus rinkos veikimą ir nėra papildoma ar netiesioginė pastarojo atžvilgiu. Todėl siūlomam reglamentui turėtų būti taikomas dvejopas pagrindas pagal atitinkamą teismo jurisprudenciją (žr. šios nuomonės 9 punktą).

36. Tačiau lieka klausimas, kuris teisinis pagrindas turėtų būti taikomas reglamentuojant asmens duomenų tvarkymą naudojant sistemas, nurodytas siūlomo reglamento 5 straipsnio 1 dalies c punkte – 5 straipsnio 4 dalyje. Iš tiesų SESV 87 straipsnio 2 dalies a punktas yra teisėsaugos tarnybų taikomų nusikalstamų veikų prevencijos, atskleidimo ir tyrimo priemonių, susijusių su svarbios informacijos rinkimu, saugojimu, tvarkymu, analize ir mainais, teisinis pagrindas.
37. Kaip generalinis advokatas paaikškino išvadoje *PNR Canada* (A1/15), tarp SESV 16 straipsnio ir SESV 87 straipsnio 2 dalies a punkto bei 82 straipsnio 1 dalies d punkto negali būti hierarchinio ryšio „*lex generalis – lex specialis*“¹⁶. SESV 16 straipsnio 2 dalis yra vienintelė nuostata, taikoma taisyklėms, susijusioms su asmenų apsauga valstybių narių teisėsaugos institucijoms tvarkant asmens duomenis nusikalstamumo prevencijos tikslais. Vien tai, kad 5 straipsnyje daroma nuoroda į Pagrindų sprendime dėl Europos arešto orderio pateiktą sunkių nusikaltimų sąrašą, šio vertinimo nekeičia: ta nuoroda nereiškia, kad tas pagrindų sprendimas yra taikytinas¹⁷. Tai tėra teisėkūros metodas, pagal kurį išvardijami sunkūs nusikaltimai, ir nėra poreikio parengti atskiro priedo.
38. Vis dėlto 5 straipsnyje nustatyta taisykle siekiama ne tiksliau apibrėžti su TVR susijusių priemonių taikymo sąlygas, o užtikrinti, kad ateityje naudojant tikrą laiką biometrinį tapatybės nustatymą DI sistemomis būtų tinkamai atsižvelgta į pagrindinių teisių klausimus, visų pirma į poreikį užtikrinti, kad biometriniai duomenys būtų renkami ir tvarkomi gerbiant teisę į privatumą ir asmens duomenis.

Šiuo atžvilgiu reglamentu nesiekama nustatyti naujos privalomos TVR skirtos procedūros, o veikiau remiamasi patikrintomis ir išbandytais procedūrinėmis priemonėmis, kad būtų užtikrinta pagarba pagrindinėms teisėms.

¹⁶ Žr. 2016 m. rugsėjo 8 d. generalinio advokato P. Mengozzi išvadą dėl Kanados ir Europos Sąjungos susitarimo projekto (Nuomonė 1/15, EU:C:2016:656, 112–120 punktai).

¹⁷ Dėl šio sunkių nusikaltimų sąrašo įgyvendinimo valstybėse narėse žr. 2022 m. birželio 21 d. Teisingumo Teismo sprendimo *Ligue des droits humains / Conseil des ministres*, C-817/19, EU:C:2022:65, 150–152 punktus.

39. Jei SESV 16 straipsnis yra tinkamas papildomas teisinis pagrindas, kyla klausimų dėl Protokolo Nr. 21 6a straipsnio ir Protokolo Nr. 22 2a straipsnio taikymo. Kaip paaiškinta pasiūlymo 25 ir 26 konstatuojamosiose dalyse, tai reiškia, kad tais atvejais, kai Airijos arba Danijos teisėsaugos institucijos naudoja tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemas viešosiose erdvėse nusikaltimų prevencijos tikslais ir kai Airijai ar Danijai nėra privalomos atitinkamos policijos bendradarbiavimo ar teismo bendradarbiavimo baudžiamosiose bylose taisyklės, toms dviem valstybėms narėms siūlomo reglamento 5 straipsnio 1 dalies d punktas, 2 ir 3 dalys nebus privalomos. Tai nereiškia, kad 5 straipsnio 1 dalies d punkte, 2 ir 3 dalyse yra pateikiamos taisyklės dėl policijos bendradarbiavimo, pavyzdžiui, taisyklės dėl teisėsaugos institucijų keitimosi informacija. Tai paprasčiausiai reiškia, kad siūlomo reglamento 5 straipsnio 1 dalies d punktu, 2 ir 3 dalimis, panašiai kaip ir Direktyva (ES) 2016/680 (Duomenų apsaugos teisėsaugos srityje direktyva), kuri yra *lex generalis*, priimta remiantis SESV 16 straipsniu, reglamentuojamas biometrinių asmens duomenų tvarkymas konkrečiomis aplinkybėmis, kai naudojamos tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos viešosiose erdvėse nusikaltimų prevencijos tikslais, ir nieko daugiau. Šiuo atžvilgiu Komisijos pasiūlyme laikomasi požiūrio, kurio Sąjungos teisės aktų leidėjas laikėsi dėl Duomenų apsaugos teisėsaugos srityje direktyvos, ir taip patvirtinama, kad šiuo atveju rėmimasis SESV 87 straipsnio 2 dalimi yra nepagrįstas.
40. SESV 16 straipsnio papildymas SESV 114 straipsniu šiuo atveju yra pagrįstas tuo, kad 5 straipsnio 1 dalies d punktas, 2 ir 3 dalys yra vieninteliai atvejai, kai reglamentuojamas leistos naudoti DI sistemos naudojimas pažeidžiant teisę į asmens duomenų apsaugą, kuri yra bendrosios duomenų apsaugos sistemos *lex specialis*. Tokios *lex specialis* duomenų apsaugos taisyklės, darančios poveikį tų jautrių DI sistemų naudojimui, negali būti laikomos papildomomis arba netiesioginėmis vidaus rinkos teisinio pagrindo atžvilgiu. Todėl SESV 16 straipsnio, kaip teisinio pagrindo, įtraukimas siūlomame reglamente yra pakankamai pagrįstas, o rėmimasis SESV 87 straipsnio 2 dalies a punktu nėra tinkamas.

IV. IŠVADA

41. Atsižvelgdama į tai, kas išdėstyta pirmiau, Tarybos Teisės tarnyba mano:

- a) rėmimasis SESV 16 ir 114 straipsniais kaip siūlomo reglamento teisiniu pagrindu yra pagrįstas ir tinkamas;
- b) rėmimasis SESV 87 straipsnio 2 dalimi ar kitu su TVR susijusiu teisiniu pagrindu nėra nei pagrįstas, nei tinkamas suderintų taisyklių, taikomų DI sistemoms, kurias gali tiekti ar naudoti teisėsaugos ar teisminės institucijos, atžvilgiu.
