EDAV-EDAPP

Bendra nuomonė Nr. 5/2021

dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas)

2021 m. birželio 18 d.

Santrauka

2021 m. balandžio 21 d. Europos Komisija pateikė pasiūlymą dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (toliau – pasiūlymas). Europos duomenų apsaugos valdyba (EDAV) ir Europos duomenų apsaugos priežiūros pareigūnas (EDAPP) palankiai vertina teisės aktų leidėjo susirūpinimą dėl dirbtinio intelekto (DI) naudojimo Europos Sąjungoje (ES) ir pabrėžia, kad pasiūlymas turi didelį **poveikį duomenų apsaugai.**

EDAV ir EDAPP pažymi, kad visų pirma pasiūlymo **teisinis pagrindas** yra Sutarties dėl Europos Sąjungos veikimo (SESV) 114 straipsnis. Be to, pasiūlymas taip pat grindžiamas SESV 16 straipsniu dėl konkrečių fizinių asmenų apsaugos taisyklių tvarkant asmens duomenis, visų pirma dėl apribojimų naudoti DI sistemas teisėsaugos tikslais nuotoliniam biometriniam tapatybės nustatymui tikruoju laiku viešosiose erdvėse. EDAV ir EDAPP primena, kad pagal ES Teisingumo Teismo (ESTT) jurisprudenciją SESV 16 straipsnyje numatytas tinkamas teisinis pagrindas tais atvejais, kai asmens duomenų apsauga yra vienas iš esminių ES teisės aktų leidėjo priimtų taisyklių tikslų ar viena iš pagrindinių šių taisyklių sudedamųjų dalių. SESV 16 straipsnio taikymas taip pat reiškia, kad **reikia užtikrinti nepriklausomą** asmens duomenų tvarkymo reikalavimų **laikymosi priežiūrą**, kaip reikalaujama ir ES pagrindinių teisių chartijos 8 straipsnyje.

Kalbant apie **pasiūlymo taikymo sritį,** EDAV ir EDAPP labai palankiai vertina, kad jį taiko ir ES institucijos, įstaigos ar agentūros teikiamoms DI sistemoms ir jų naudojimui. Tačiau tai, kad į **pasiūlymo taikymo sritį neįtrauktas tarptautinis teisėsaugos institucijų bendradarbiavimas**, kelia didelį susirūpinimą EDAV ir EDAPP, nes dėl tokios išimties kyla didelė priemonių vengimo rizika (pvz., trečiosiose šalyse arba tarptautinėse organizacijose, naudojančiose didelės rizikos taikomąsias programas, kuriomis grindžiamas ES valdžios institucijų darbas).

EDAV ir EDAPP **palankiai vertina rizika grindžiamą požiūrį**, kuriuo paremtas pasiūlymas. Tačiau šis požiūris turėtų būti paaiškintas, o sąvoka „pavojus pagrindinėms teisėms“ turėtų būti suderinta su Bendruoju duomenų apsaugos reglamentu (BDAR) ir Reglamentu (ES) 2018/1725 (ESDAR), nes atsiranda su asmens duomenų apsauga susijusių aspektų.

Be to, EDAV ir EDAPP sutinka su pasiūlymu, kad **DI sistemos priskyrimas didelės rizikos kategorijai nebūtinai reiškia, kad ji savaime yra teisėta** ir naudotojas gali ją naudoti kaip tokią. Duomenų valdytojui gali reikėti laikytis **ir kitų ES duomenų apsaugos teisės aktuose nustatytų reikalavimų**. Be to, laikytis teisinių įsipareigojimų pagal Sąjungos teisės aktus (įskaitant asmens duomenų apsaugą) turėtų būti privaloma, jei gaminys Europos rinkoje žymimas CE ženklu. Todėl EDAV ir EDAPP mano, jog **reikalavimas užtikrinti, kad būtų laikomasi BDAR ir ESDAR nuostatų, turėtų būti įtrauktas į III antraštinės dalies 2 skyrių**. Be to, EDAV ir EDAPP mano, kad pasiūlymo atitikties vertinimo procedūrą reikia pritaikyti taip, kad trečiosios šalys visada turėtų atlikti didelės rizikos DI sistemų *ex ante* atitikties vertinimus.

Atsižvelgiant į didelę diskriminavimo riziką, pasiūlyme draudžiamas „socialinis vertinimas“, kai tai daroma „tam tikrą laikotarpį“ arba jis atliekamas „valdžios institucijų ar jų vardu“. Tačiau privačios bendrovės, pvz., socialinės žiniasklaidos ir debesijos paslaugų teikėjai, taip pat gali tvarkyti didelius asmens duomenų kiekius ir atlikti socialinius įvertinimus. Todėl **būsimame DI reglamente turėtų būti uždraustas bet kokios rūšies socialinis vertinimas.**

Nuotolinis biometrinis asmenų tapatybės nustatymas viešosiose erdvėse kelia didelį įsibrovimo į asmeninį gyvenimą pavojų, o tai daro didelį poveikį gyventojų lūkesčiams būti anonimiškiems viešosiose erdvėse.

Dėl šių priežasčių EDAV ir EDAPP ragina bet kokiomis aplinkybėmis **apskritai uždrausti naudoti DI automatiniam žmogaus savybių atpažinimui viešosiose erdvėse**, pavyzdžiui, veido, taip pat eisenos, pirštų atspaudų, DNR, balso, spausdinimo klaviatūra ir kitų biometrinių ar elgesio signalų. Taip pat rekomenduojama **uždrausti DI sistemas, pagal kurias asmenys iš biometrinių duomenų skirstomi į grupes** pagal etninę kilmę, lytį, politinę ar seksualinę orientaciją arba kitus diskriminacijos pagrindus pagal Chartijos 21 straipsnį. Be to, EDAV ir EDAPP mano, kad DI naudojimas **siekiant numatyti fizinio asmens emocijas yra ypač nepageidautinas ir turėtų būti uždraustas.**

EDAV ir EDAPP palankiai vertina tai, kad **pasiūlyme EDAPP paskirtas kompetentinga institucija ir rinkos priežiūros institucija, kuri atsakinga už Sąjungos institucijų, agentūrų ir įstaigų priežiūrą.** Tačiau reikėtų išsamiau paaiškinti EDAPP funkcijas ir užduotis, ypač jo, kaip rinkos priežiūros institucijos, vaidmenį. Be to, būsimame DI reglamente turėtų būti aiškiai nustatytas **priežiūros institucijų nepriklausomumas** vykdant priežiūros ir vykdymo užtikrinimo užduotis.

Paskyrus duomenų apsaugos institucijas (DAI) nacionalinėmis priežiūros institucijomis būtų užtikrintas labiau suderintas reguliavimas, padedama nuosekliau aiškinti duomenų tvarkymo nuostatas ir išvengiama prieštaravimų užtikrinant jų vykdymą valstybėse narėse. Todėl EDAV ir EDAPP mano, kad **pagal pasiūlymo 59 straipsnį duomenų apsaugos institucijos turėtų būti paskirtos nacionalinėmis priežiūros institucijomis.**

Pasiūlyme Komisijai suteikiamas pagrindinis vaidmuo Europos dirbtinio intelekto valdyboje (EDIV). Toks vaidmuo prieštarauja būtinybei, kad DI Europos įstaiga būtų nepriklausoma nuo bet kokios politinės įtakos. Siekiant užtikrinti būsimo DI reglamento nepriklausomumą, **EDIV turėtų būti suteikta daugiau savarankiškumo** ir užtikrinama, kad ji galėtų veikti savo iniciatyva.

Atsižvelgiant į DI sistemų paplitimą bendrojoje rinkoje ir tarpvalstybinių bylų tikimybę, itin svarbu suderinti vykdymo užtikrinimą ir tinkamai paskirstyti nacionalinių priežiūros institucijų kompetenciją. EDAV ir EDAPP siūlo numatyti **mechanizmą, pagal kurį įmonėms ir asmenims, kuriems taikomi teisės aktai, būtų užtikrintas vienas bendras informacinis punktas pagal kiekvieną DI sistemą.**

EDAV ir EDAPP taip pat **rekomenduoja patikslinti bandomosios aplinkos taikymo sritį ir tikslus.** Pasiūlyme taip pat turėtų būti aiškiai nurodyta, kad teisinis tokios bandomosios aplinkos pagrindas turėtų atitikti esamos duomenų apsaugos sistemos reikalavimus.

Pasiūlyme išdėstyta **sertifikavimo sistema nėra aiškiai susieta su ES duomenų apsaugos teise**, taip pat su kitais ES ir valstybių narių teisės aktais, kurie yra taikomi kiekvienai didelės rizikos DI sistemos sričiai, ir joje neatsižvelgiama į **duomenų kiekio mažinimo ir pritaikytosios duomenų apsaugos principus** kaip į vieną iš aspektų, į kuriuos reikia atsižvelgti **prieš gaunant CE ženklą.** Todėl EDAV ir EDAPP rekomenduoja iš dalies pakeisti pasiūlymą, kad būtų patikslintas pagal minėtą reglamentą išduotų sertifikatų ir duomenų apsaugos sertifikatų, ženklų ir žymenų santykis. Galiausiai, duomenų apsaugos institucijos turėtų dalyvauti rengiant ir nustatant darniuosius standartus ir bendrąsias specifikacijas.

Dėl **elgesio kodeksų** EDAV ir EDAPP mano, kad **būtina paaiškinti**, ar asmens duomenų apsauga turi būti laikoma vienu iš „papildomų reikalavimų“, kuriuos galima įtraukti į šiuos elgesio kodeksus, ir užtikrinti, kad „techninės specifikacijos ir sprendimai“ neprieštarautų ES duomenų apsaugos sistemos taisyklėms ir principams.

TURINYS

Europos duomenų apsaugos valdyba ir Europos duomenų apsaugos priežiūros pareigūnas

atsižvelgdami į 2018 m. spalio 23 d. Reglamentą 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB[1],

atsižvelgdami į EEE susitarimą, ypač į jo XI priedą ir 37 protokolą su pakeitimais, padarytais 2018 m. liepos 6 d. EEE jungtinio komiteto sprendimu Nr. 154/2018[2],

atsižvelgdami į 2021 m. balandžio 22 d. Europos duomenų apsaugos priežiūros pareigūno ir Europos duomenų apsaugos valdybos prašymą pateikti bendrą nuomonę dėl reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas), pasiūlymo,

PRIĖMĖ ŠIĄ BENDRĄ NUOMONĘ

1 ĮVADAS

1. Dirbtinio intelekto (DI) sistemų atsiradimas yra labai svarbus technologijų raidos ir žmonių sąveikos su jomis etapas. Dirbtinis intelektas yra pagrindinių technologijų rinkinys, kuris iš esmės pakeis mūsų kasdienį gyvenimą tiek socialiniu, tiek ekonominiu požiūriu. Tikimasi, kad artimiausiu metu bus priimti esminiai su dirbtiniu intelektu susiję sprendimai, padėsiantys mums įveikti kai kuriuos didžiausius iššūkius, su kuriais šiandien susiduriame daugelyje sričių – tiek sveikatos priežiūros ir judumo, tiek viešojo administravimo ir švietimo.

2. Tačiau ši viliojanti pažanga kelia įvairių pavojų. Iš tiesų pavojai yra netgi labai realūs, kadangi beveik nėra patirties, kokį poveikį DI sistemos gali daryti asmeniui ir visuomenei. Automatizuotas turinio kūrimas, prognozavimas ar sprendimo priėmimas, kuriuos atlieka dirbtinio intelekto sistemos, taikydamos mašinų mokymosi metodus arba logines ir tikimybines išvadas, nėra tas pats, kai tą veiklą vykdo žmonės, pasitelkdami kūrybinius ar teorinius argumentus ir prisiimantys visą atsakomybę už pasekmes.

3. Dirbtinis intelektas padidins prognozių, kurias galima atlikti daugelyje sričių, skaičių, pradedant nuo išmatuojamų duomenų sąsajų, kurios nematomos žmogaus akims, bet matomos mašinoms, – tai palengvins mūsų gyvenimą ir išspręs daug problemų, tačiau tuo pačiu mažins mūsų gebėjimą suprasti pasekmių priežastis, o tai kels pavojų skaidrumui, žmogaus vykdomai kontrolei, atskaitomybei ir atsakomybei už rezultatus.

[1] OL L 295, 2018 11 21, p. 39–98.
[2] Šiame dokumente daromos nuorodos į valstybes nares turėtų būti suprantamos kaip nuorodos į EEE valstybes nares.

4. DI duomenys (asmens ir ne asmens) daugeliu atveju yra pagrindinė prielaida, kuria remiantis priimami savarankiški sprendimai, o tai neišvengiamai paveiks asmenų gyvenimą įvairiais lygmenimis. Todėl Europos duomenų apsaugos valdyba ir EDAPP jau šiame etape tvirtina, kad pasiūlymas dėl reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas, toliau – pasiūlymas)[3], turi **svarbių pasekmių duomenų apsaugai.**

5. Suteikus mašinoms teisę priiminėti sprendimus remiantis duomenimis, kiltų pavojus asmenų teisėms ir laisvėms, atsirastų poveikis jų asmeniniam gyvenimui, galėtų būti padaryta žala grupėms ar net visai visuomenei. EDAV ir EDAPP pabrėžia, kad teisės į privatų gyvenimą ir į asmens duomenų apsaugą, prieštaraujančios mašinų sprendimų savarankiškumo prielaidai, kuria grindžiama DI sąvoka, yra ES vertybių, pripažintų Visuotinėje žmogaus teisių deklaracijoje (12 straipsnis), Europos žmogaus teisių konvencijoje (8 straipsnis) ir ES pagrindinių teisių chartijoje (toliau – Chartija) (7 ir 8 straipsniai), ramstis. Labai ambicingas, tačiau būtinas tikslas – suderinti dirbtinio intelekto taikomųjų programų augimo perspektyvą ir žmonių svarbą bei viršenybę mašinų atžvilgiu.

6. EDAV ir EDAPP palankiai vertina tai, kad visi DI vertės grandinės suinteresuotieji subjektai dalyvauja reglamentavimo procese ir kad nustatyti konkretūs reikalavimai sprendimų teikėjams, nes jie atlieka svarbų su jų sistemose naudojamais produktais susijusį vaidmenį. Tačiau reikia aiškiai apibrėžti ir priskirti įvairių šalių – DI sistemos naudotojo, teikėjo, importuotojo ar platintojo – atsakomybę. Visų pirma, tvarkant asmens duomenis, ypatingas dėmesys turėtų būti skiriamas šių funkcijų ir atsakomybės derėjimui su duomenų apsaugos sistemoje vartojamomis duomenų valdytojo ir duomenų tvarkytojo sąvokomis, nes abi normos nesutampa.

7. Pasiūlyme teikiama didelė reikšmė žmogaus vykdomos priežiūros sąvokai (14 straipsnis), kurią palankiai vertina EDAV ir EDAPP. Tačiau, kaip nurodyta pirmiau, dėl didelio galimo tam tikrų dirbtinio intelekto sistemų poveikio asmenims ar asmenų grupėms, tikrasis žmogiškasis sprendimo priėmimo principas turėtų remtis aukštos kvalifikacijos žmogaus atliekama priežiūra ir teisėtu duomenų tvarkymu, jei tokios sistemos grindžiamos asmens duomenų tvarkymu arba tvarko asmens duomenis, siekiant atlikti numatytą užduotį, – taip būtų užtikrinama pagarba teisei netapti vien automatizuoto duomenų tvarkymo pagrindu priimto sprendimo subjektu.

8. Be to, atsižvelgiant į tai, kad daugeliui DI taikomųjų programų reikia daug duomenų, pasiūlymu turėtų būti skatinama visais lygmenimis taikyti pritaikytosios ir standartizuotosios duomenų apsaugos metodą, skatinant veiksmingai įgyvendinti duomenų apsaugos principus (kaip numatyta BDAR 25 straipsnyje ir ESDAR 27 straipsnyje) naudojant naujausias technologijas.

9. Galiausiai EDAV ir EDAPP pabrėžia, kad ši bendra nuomonė pateikiama tik kaip preliminari pasiūlymo analizė, nedarant poveikio tolesniems pasiūlymo poveikio vertinimams ir nuomonėms ir jo suderinamumui su ES duomenų apsaugos teise.

[3] COM(2021) 206 *final*.

2 PAGRINDINIŲ PASIŪLYMO PRINCIPŲ ANALIZĖ

2.1 Pasiūlymo taikymo sritis ir ryšys su galiojančia teisine sistema

10. Remiantis aiškinamuoju memorandumu, pasiūlymo **teisinis pagrindas** visų pirma yra SESV 114 straipsnis, kuriame numatoma taikyti vidaus rinkos sukūrimą ir veikimą užtikrinančias priemones[4]. Be to, pasiūlyme remiamasi SESV 16 straipsniu *dėl konkrečių fizinių asmenų apsaugos taisyklių tvarkant asmens duomenis*, visų pirma dėl apribojimų naudoti dirbtinio intelekto sistemas teisėsaugos tikslais nuotoliniam biometriniam tapatybės nustatymui tikruoju laiku viešosiose erdvėse[5].

11. EDAV ir EDAPP primena, kad pagal ESTT praktiką SESV 16 straipsnyje numatomas tinkamas teisinis pagrindas tais atvejais, kai asmens duomenų apsauga yra vienas iš esminių ES teisės aktų leidėjo priimtų taisyklių tikslų ar viena iš esminių šių taisyklių sudedamųjų dalių[6]. SESV 16 straipsnio taikymas taip pat reiškia, kad reikia užtikrinti nepriklausomą priežiūrą, kaip laikomasi asmens duomenų tvarkymo reikalavimų, kaip numatoma ir Chartijos 8 straipsnyje.

12. EDAPP ir EDAV primena, kad jau egzistuoja išsami duomenų apsaugos sistema, priimta remiantis SESV 16 straipsniu, kurią sudaro BDAR[7], Europos Sąjungos institucijoms, tarnyboms, organams ir agentūroms skirtas Duomenų apsaugos reglamentas (ESDAR)[8] ir Teisėsaugos direktyva (TD)[9]. Pagal pasiūlymą tik papildomi pasiūlyme nustatyti biometrinių duomenų tvarkymo apribojimai gali būti laikomi grindžiamais SESV 16 straipsniu ir todėl turintys tokį patį teisinį pagrindą kaip BDAR, ESDAR ar TD. Tai daro svarbų poveikį pasiūlymo sąsajoms su BDAR, ESDAR ir apskritai TD, kaip nurodyta toliau.

13. Dėl **pasiūlymo taikymo srities** pažymėtina, kad EDAV ir EDAPP labai palankiai vertina tai, kad pasiūlyme numatytas ES institucijų, organų ar agentūrų DI sistemų naudojimas. Atsižvelgiant į tai, kad šių subjektų naudojimasis DI sistemomis taip pat gali turėti didelį poveikį pagrindinėms asmenų teisėms, panašiai kaip ir ES valstybėse narėse, būtina, kad naujoji DI reguliavimo sistema būtų taikoma ir ES valstybėms narėms, ir ES institucijoms, tarnyboms, organams ir agentūroms, siekiant užtikrinti nuoseklų požiūrį visoje Sąjungoje. Kadangi ES institucijos, tarnybos, organai ir agentūros gali veikti ir kaip DI sistemų teikėjai ir

[4] Aiškinamasis memorandumas, 5 psl.
[5] Aiškinamasis memorandumas, 6 psl. Žr. pasiūlymo 2 konstatuojamąją dalį.
[6] 2017 m. liepos 26 d. nuomonė dėl *PNR Kanada*, Nuomonės procedūra 1/15, ECLI:EU:C:2017:592, 96 punktas.
[7] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1–88).
[8] 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39–98).
[9] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016 5 4, p. 89–131).

naudotojai, EDAPP ir EDAV mano, kad visiškai tikslinga įtraukti šiuos subjektus į pasiūlymo taikymo sritį remiantis SESV 114 straipsniu.

14. Tačiau EDAV ir EDAPP didelį susirūpinimą kelia tai, kad tarptautinis bendradarbiavimas teisėsaugos srityje nepatenka į pasiūlymo 2 straipsnio 4 dalyje nustatytą taikymo sritį. Dėl šios išimties kyla didelė priemonių vengimo rizika (pvz., trečiosiose šalyse arba tarptautinėse organizacijose, naudojančiose didelės rizikos taikomąsias programas, kuriomis grindžiamas ES valdžios institucijų darbas).

15. DI sistemų kūrimas ir naudojimas daugeliu atvejų bus susijęs su asmens duomenų tvarkymu. Itin svarbu užtikrinti šio pasiūlymo ir galiojančių ES teisės aktų dėl duomenų apsaugos aiškumą. Pasiūlymas nedaro poveikio BDAR, ESDAR ir TD ir juos papildo. Nors pasiūlymo konstatuojamosiose dalyse paaiškinta, kad DI sistemų naudojimas vis tiek turėtų atitikti duomenų apsaugos teisę, **EDAV ir EDAPP primygtinai rekomenduoja pasiūlymo 1 straipsnyje paaiškinti**, kad bet kokiam į pasiūlymo taikymo sritį patenkančiam asmens duomenų tvarkymui būtų **taikomi Sąjungos teisės aktai dėl asmens duomenų apsaugos**, visų pirma BDAR, ESDAR, E. privatumo direktyva[10] ir TD. Atitinkamoje konstatuojamoje dalyje taip pat turėtų būti paaiškinta, kad pasiūlymu nesiekiama daryti poveikio galiojančių ES teisės aktų, kuriais reglamentuojamas asmens duomenų tvarkymas, taikymui, įskaitant nepriklausomų priežiūros institucijų, kurios kompetentingos stebėti, kaip tų aktų laikomasi, užduotis ir įgaliojimus.

2.2 Rizika grindžiamas požiūris

16. EDAV ir EDAPP **palankiai vertina rizika grindžiamą požiūrį**, kuriuo paremtas pasiūlymas. Pasiūlymas būtų taikomas visoms DI sistemoms, įskaitant nesusijusias su asmens duomenų tvarkymu, tačiau vis tiek gali daryti poveikį interesams arba pagrindinėms teisėms bei laisvėms.

17. EDAV ir EDAPP atkreipia dėmesį į tai, kad pagal kai kurias pasiūlymo nuostatas panaikinama rizika asmenų grupėms ar visai visuomenei (pvz., ypatingos svarbos kolektyvinį poveikį – grupių diskriminaciją ar politinių nuomonių reiškimą viešosiose erdvėse). EDAV ir EDAPP rekomenduoja, kad taip pat būtų įvertinta ir sumažinta DI sistemų keliama socialinė rizika asmenų grupėms.

18. EDAV ir EDAPP laikosi nuomonės, kad turėtų būti patikslintas pasiūlymo rizika grindžiamas požiūris, o sąvoka „pavojus pagrindinėms teisėms“ turėtų būti **suderinta su BDAR**, atsižvelgiant į aspektus, susijusius su asmens duomenų apsauga. Nepaisant to, ar jie yra galutiniai naudotojai, tiesiog duomenų subjektai ar kiti asmenys, susiję su DI sistema, pasiūlyme nėra nuorodos į asmenį, kuriam DI sistema daro poveikį. Iš tiesų subjektų pareigos susijusių asmenų atžvilgiu turėtų būti konkrečiau susietos su asmens ir jo teisių apsauga. Todėl EDAV ir EDAPP ragina teisės aktų leidėjus pasiūlyme aiškiai nurodyti asmenų, kuriems taikomos DI sistemos, **teises ir teisių gynimo priemones**.

[10] 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) su pakeitimais, padarytais Direktyva 2006/24/EB ir Direktyva 2009/136/EB.

19. EDAV ir EDAPP atsižvelgia į pasirinkimą pateikti išsamų **didelės rizikos DI sistemų** sąrašą. Šis pasirinkimas gali lemti ribotą poveikį, esant mažai labai rizikingų situacijų pritraukimo tikimybei. Todėl bendras rizika grindžiamas požiūris, kuriuo paremtas pasiūlymas, nebetektų prasmės. Be to, pasiūlymo II ir III prieduose pateiktame didelės rizikos DI sistemų sąraše nėra kai kurių naudojimo atvejų, susijusių su didele rizika, pavyzdžiui, dirbtinio intelekto naudojimas draudimo įmokoms nustatyti, medicininiam gydymui vertinti arba sveikatos tyrimams atlikti. EDAV ir EDAPP taip pat pabrėžia, kad tuos priedus reikės reguliariai atnaujinti, siekiant užtikrinti tinkamą jų taikymo sritį.

20. Pasiūlyme reikalaujama, kad DI sistemos **teikėjai** atliktų rizikos vertinimą, tačiau daugeliu atvejų (duomenų) valdytojai bus DI sistemų **naudotojai**, o ne teikėjai (pvz., veido atpažinimo sistemos naudotojas yra duomenų valdytojas, todėl jam netaikomi pasiūlyme nustatyti didelės rizikos dirbtinio intelekto teikėjams keliami reikalavimai).

21. Be to, **paslaugų teikėjas ne visada galės įvertinti visus** DI sistemos **naudojimo būdus.** Taigi pradinis rizikos vertinimas bus bendresnio pobūdžio nei DI sistemos naudotojo atliekamas vertinimas. Net jei iš paslaugų teikėjo pirminio rizikos vertinimo nematyti, kad DI sistema pagal pasiūlymą yra „didelės rizikos“, dėl to neturėtų būti atmetama galimybė atlikti **paskesnį (išsamesnį) vertinimą** (poveikio duomenų apsaugai vertinimas pagal BDAR 35 straipsnį, ESDAR 39 straipsnį arba TD 27 straipsnį), kurį **turėtų atlikti sistemos naudotojas**, atsižvelgdamas į naudojimo aplinkybes ir konkrečius naudojimo atvejus. Aiškinimas, ar pagal BDAR, ESDAR ir TD tam tikros rūšies duomenų tvarkymas gali kelti didelę riziką, turi būti atliekamas nepriklausomai nuo pasiūlymo. Tačiau tai, kad DI sistema klasifikuojama kaip kelianti didelę riziką dėl jos poveikio pagrindinėms teisėms,[11] **reiškia didelės rizikos prielaidą pagal BDAR, ESDAR ir TD tais atvejais, kai tvarkomi asmens duomenys.**

22. **Be to, EDAV ir EDAPP sutinka su pasiūlymu, kad DI sistemos priskyrimas didelės rizikos kategorijai nebūtinai reiškia, kad ji savaime yra teisėta ir naudotojas gali ją naudoti kaip tokią. Duomenų valdytojui gali reikėti laikytis kitų ES duomenų apsaugos teisės aktuose nustatytų reikalavimų.** Be to, pasiūlymo 5 straipsnio pagrindimas, kad, skirtingai nuo draudžiamų sistemų, didelės rizikos sistemos iš esmės gali būti leidžiamos, turi būti nagrinėjamas ir pašalintas iš pasiūlymo, juo labiau, kad siūlomas CE ženklas nereiškia, kad susijęs asmens duomenų tvarkymas yra teisėtas.

23. Tačiau Sąjungos teisės aktuose nustatytų reikalavimų (įskaitant asmens duomenų apsaugą) laikymasis turėtų būti privalomas, siekiant Europos rinkai pateikti CE ženklu pažymėtus gaminius. Todėl EDAV ir EDAPP **rekomenduoja į pasiūlymo III antraštinės dalies 2 skyrių įtraukti reikalavimą užtikrinti BDAR ir ESDAR nuostatų laikymąsi.** Šie reikalavimai audituojami (atliekant trečiosios šalies auditą) prieš ženklinimą CE ženklu, laikantis

[11]Europos Sąjungos pagrindinių teisių agentūra (FRA) jau atsižvelgė į poreikį atlikti poveikio pagrindinėms teisėms vertinimus naudojant dirbtinį intelektą ar susijusias technologijas. 2020 m. ataskaitoje „Teisės ateityje. Dirbtinis intelektas ir pagrindinės teisės“ FRA nustatė „pavojus dėl dirbtinio intelekto naudojimo, pavyzdžiui, prognozuojant viešosios tvarkos palaikymą, teikiant medicinines diagnozes, socialines paslaugas ir tikslinę reklamą“, ir pabrėžė, kad siekiant sumažinti neigiamą poveikį asmenims „privačios ir viešosios organizacijos turėtų atlikti vertinimus, kaip dirbtinis intelektas galėtų pakenkti pagrindinėms teisėms“.

atskaitomybės principo. Atsižvelgiant į šį trečiosios šalies vertinimą, pradinis poveikio vertinimas, kurį turi atlikti paslaugų teikėjas, bus ypač svarbus.

24. Atsižvelgiant į DI sistemų kūrimo sukeltus sunkumus, reikėtų pažymėti, kad dėl DI sistemų techninių savybių (pvz., DI metodo rūšies) gali kilti didesnė rizika. Todėl atliekant bet kokį DI sistemos rizikos vertinimą reikėtų atsižvelgti į **technines charakteristikas**, **konkrečius jos naudojimo atvejus ir aplinkybes**, kuriomis sistema veikia.

25. Atsižvelgdami į tai, kas išdėstyta pirmiau, EDAV ir EDAPP rekomenduoja pasiūlyme nurodyti, kad **paslaugų teikėjas** turi atlikti pradinį atitinkamos DI sistemos rizikos vertinimą, **atsižvelgdamas į naudojimo atvejus** (kurie turi būti nurodyti pasiūlyme, papildant, pavyzdžiui, III priedo 1 dalies a punktą, kuriame DI biometrinių sistemų naudojimo atvejai neminimi), ir kad DI sistemos **naudotojas** pagal ES duomenų apsaugos teisės aktais (jei taikoma) nustatytus reikalavimus duomenų valdytojui, atlieka poveikio duomenų apsaugai vertinimą pagal BDAR 35 straipsnį, ESDAR 39 straipsnį ir TD 27 straipsnį, atsižvelgdamas ne vien į techninę charakteristiką ir **naudojimo atvejus**, tačiau ir į **konkrečią aplinką**, kurioje DI veikia.

26. Be to, turėtų būti paaiškintos kai kurios pasiūlymo III priede nurodytos sąvokos, pvz., terminas „pagrindinės privačios paslaugos“ arba smulkus paslaugų teikėjas, naudojantis DI kreditingumo vertinimą savo reikmėms.

2.3 Draudžiamas DI naudojimas

27. EDAV ir EDAPP mano, kad **invazinės dirbtinio intelekto formos**, ypač tos, kurios gali daryti poveikį žmogaus orumui, turi būti laikomos draudžiamomis DI sistemomis pagal pasiūlymo 5 straipsnį, o ne tiesiog pasiūlymo III priede priskiriamos prie didelės rizikos, kaip nurodyta 6 punkte. Tai visų pirma taikoma duomenų palyginimams, kurie dideliu mastu taip pat daro poveikį asmenims, nenurodžiusiems policijos stebėjimo priežasčių arba nurodytos priežastys yra nesvarios, arba duomenų tvarkymui, kuriuo pažeidžiamas duomenų apsaugos teisės aktuose nustatytas tikslo apribojimo principas. Norint naudoti dirbtinį intelektą policijos ir teisėsaugos srityje, reikalingos konkrečios srities, tikslios, numatomos ir proporcingos taisyklės, kuriomis turi būti atsižvelgiama į atitinkamų asmenų interesus ir poveikį demokratinės visuomenės veikimui.

28. Kyla pavojus, kad pasiūlymo 5 straipsnyje nurodytos nuostatos ir DI sistemų uždraudimas nebus įgyvendintas. Iš tiesų pagal 5 straipsnyje nurodytus kriterijus, kuriais remiantis dirbtinio intelekto sistemos gali būti uždraustos, **draudimo taikymas ribojamas** tokiu mastu, kad realybėje toks uždraudimas gali nebetekti prasmės (pvz., 5 straipsnio 1 dalies a ir b punktuose nurodytos „priežastys arba galimybės sukelti [...] fizinę ar psichologinę žalą“; 5 straipsnio 1 dalies c punkte nurodyti apribojimai valdžios institucijoms; miglota c punkto ir jo i ir ii papunkčių formuluotė; tik nuotolinis biometrinis tapatybės nustatymas tikruoju laiku, nepateikiant jokios aiškios apibrėžties ir pan.).

29. Visų pirma, DI naudojimas „socialiniam vertinimui“, kaip numatyta pasiūlymo 5 straipsnio 1 dalies c punkte, gali lemti diskriminaciją ir prieštarauja ES pagrindinėms vertybėms. Pasiūlyme tokia praktika draudžiama tik tada, kai yra vykdoma „tam tikrą laikotarpį“ arba kai ją vykdo „valdžios institucijos arba ji vykdoma jų vardu“. Uždarosios akcinės bendrovės, visų pirma socialinės žiniasklaidos ir debesijos paslaugų teikėjai, gali tvarkyti didelius asmens duomenų kiekius ir atlikti socialinius vertinimus. Todėl **pasiūlymu turėtų būti draudžiamas bet kokios rūšies socialinis vertinimas.** Reikėtų pažymėti, kad teisėsaugos srityje TD 4 straipsniu jau dabar gerokai apribojama, o gal net praktiškai draudžiama tokios rūšies veikla.

30. **Nuotolinis biometrinis asmenų tapatybės nustatymas** viešosiose erdvėse kelia didelį įsibrovimo į asmeninį gyvenimą pavojų. Todėl EDAV ir EDAPP **mano, kad būtinas griežtesnis požiūris.** Naudojant DI sistemas, gali kilti rimtų proporcingumo problemų, nes tai gali būti susiję su nediferencijuoto ir neproporcingo duomenų subjektų skaičiaus duomenų tvarkymu siekiant nustatyti tik kelis asmenis (pvz., keleivius oro uostuose ir traukinių stotyse). Dėl **neriboto** nuotolinio biometrinio tapatybės nustatymo sistemų veikimo pobūdžio taip pat kyla keblumų, susijusių su skaidrumo principu bei dėl teisinio duomenų tvarkymo pagrindo pagal ES teisę (TD, BDAR, ESDAR ir kitus taikytinus teisės aktus). Vis dar neišspręsta problema, kaip tinkamai informuoti asmenis apie tokį duomenų tvarkymą, o taip pat ir kaip veiksmingai ir laiku užtikrinti asmens teises. Tas pats pasakytina apie **negrįžtamą ir rimtą poveikį** (pagrįstiems) **gyventojų lūkesčiams, kad viešosiose erdvėse jie yra anonimiški**, o tai turės tiesioginį neigiamą poveikį saviraiškos, susirinkimų rengimo ir jungimosi į asociacijas bei judėjimo laisvei.

31. Pasiūlymo 5 straipsnio 1 dalies d punkte pateikiamas išsamus **išskirtinių atvejų sąrašas**, kai teisėsaugos tikslais leidžiama tikruoju laiku atlikti nuotolinį biometrinį tapatybės nustatymą viešosiose erdvėse. EDAV ir EDAPP mano, kad **šis požiūris turi trūkumų** keliais aspektais: Pirma, neaišku, ką reikėtų suprasti kaip „reikšmingą vėlavimą“ ir kodėl jis turėtų būti laikomas švelninančiu veiksniu, atsižvelgiant į tai, kad masinio identifikavimo sistema gali nustatyti tūkstančius asmenų vos per kelias valandas. Be to, duomenų tvarkymo invaziškumas ne visada priklauso nuo to, ar tapatybė nustatoma tikruoju laiku, ar ne. Nuotolinis paskesnis biometrinis tapatybės nustatymas politinio protesto metu gali turėti didelį atgrasomąjį poveikį naudojimuisi pagrindinėmis teisėmis ir laisvėmis, pavyzdžiui, susirinkimų ir asociacijų laisve ir apskritai remtis pagrindiniais demokratijos principais. Antra, duomenų tvarkymo invaziškumas nebūtinai priklauso nuo jo tikslo. Šios sistemos naudojimas kitiems tikslams, pavyzdžiui, privačiam saugumui, kelia tą pačią grėsmę pagrindinėms teisėms – teisei į privatų ir šeimos gyvenimą ir asmens duomenų apsaugai. Galiausiai, net ir esant numatytiems apribojimams, galimas įtariamųjų arba nusikaltimų vykdytojų skaičius beveik visada bus pakankamas, kad būtų galima pateisinti nuolatinį dirbtinio intelekto sistemų naudojimą įtariamiesiems nustatyti, nepaisant papildomų pasiūlymo 5 straipsnio 2–4 dalyse nustatytų sąlygų. Atrodo, kad pasiūlyme neatsižvelgiama į tai, kad vykdant atvirų erdvių stebėseną ES duomenų apsaugos teisės aktuose nustatyti įpareigojimai turi būti vykdomi ne tik įtariamiesiems, bet ir visiems, kurie praktiškai stebimi.

32. Dėl visų šių priežasčių EDAV ir EDAPP **ragina bet kokiomis aplinkybėmis apskritai uždrausti naudoti DI siekiant automatiškai atpažinti žmogaus savybes viešosiose erdvėse, pavyzdžiui, veidus, o taip pat eiseną, pirštų atspaudus, DNR, balsą, spausdinimo klaviatūra ir kitus biometrinius ar elgesio signalus**. Dabartinis pasiūlymo metodas – nustatyti ir išvardyti visas DI sistemas, kurios turėtų būti uždraustos. Todėl, siekiant nuoseklumo, pagal pasiūlymo 5 straipsnį turėtų būti draudžiamos **DI sistemos, skirtos didelio masto nuotoliniam tapatybės nustatymui interneto erdvėse**. Atsižvelgdami į TD, ESDAR ir BDAR, EDAPP ir EDAV negali nustatyti, kaip tokia praktika galėtų atitikti būtinumo ir proporcingumo reikalavimus, o tam galiausiai įtakos turi tai, kokios ESTT ir EŽTT siūlomos su pagrindinėmis teisėmis susijusios priemonės laikomos priimtinomis.

33. Be to, EDAV ir EDAPP **rekomenduoja uždrausti** tiek valdžios institucijoms, tiek privatiems subjektams DI sistemas, pagal kurias asmenys iš biometrinių duomenų **(pavyzdžiui, pagal veido atpažinimą) skirstomi į grupes pagal etninę kilmę, lytį, politinę ar seksualinę orientaciją arba kitus diskriminacijos pagrindus, draudžiamus pagal Chartijos 21 straipsnį**, arba DI sistemas, kurių mokslinis pagrįstumas nėra įrodytas arba kurios tiesiogiai prieštarauja esminėms ES vertybėms (pvz., poligrafija, III priedo 6 dalies b punktas ir 7 dalies a punktas). Todėl **biometrinis skirstymas į kategorijas** turėtų būti **uždraustas pagal 5 straipsnį.**

34. Be to, kai **būsimas elgesys nustatomas ar priskiriamas tam tikrai kategorijai kompiuteriu, neatsižvelgiant į žmogaus laisvą pasirinkimą, daromas poveikis žmogaus orumui.** DI sistemos, kurias teisėsaugos institucijos ketina naudoti atlikdamos individualius fizinių asmenų rizikos vertinimus, siekiant nustatyti fizinio asmens pakartotinės nusikalstamos veikos riziką, plg. III priedo 6 punktą. a) arba numatyti faktines ar galimas nusikalstamas veikas ar jų pasikartojimą, remiantis fizinio asmens profiliavimu arba asmenybės savybių ir charakteristikų ar buvusio nusikalstamo elgesio vertinimu, plg. III priedo 6 punktą. e) naudojant pagal numatytą paskirtį, policijos ir teismo sprendimų priėmimas taps iš esmės priklausomas, o tai sudaiktins asmenis, kuriems daromas poveikis. Tokios DI sistemos, kuriomis daromas poveikis teisėms į žmogaus orumą, turėtų būti draudžiamos pagal 5 straipsnį.

35. Be to, EDAV ir EDAPP mano, kad DI naudojimas, siekiant **numatyti fizinio asmens emocijas, yra labai nepageidautinas ir turėtų būti uždraustas**, išskyrus tam tikrus aiškiai apibrėžtus naudojimo atvejus, t. y. kai naudojamas sveikatos ar mokslinių tyrimų tikslais (pvz., pacientams, kuriems svarbu atpažinti emocijas), visada taikant tinkamas apsaugos priemones ir, žinoma, laikantis visų kitų duomenų apsaugos sąlygų ir apribojimų, įskaitant tikslų ribojimą.

2.4 Didelės rizikos DI sistemos

2.4.1 Poreikis atlikti išorės trečiųjų šalių *ex ante* atitikties vertinimą

36. EDAV ir EDAPP palankiai vertina tai, kad didelę riziką keliančioms DI sistemoms, prieš jas pateikiant rinkai ar kitaip pradedant eksploatuoti ES, turi būti atliktas išankstinis atitikties vertinimas. Iš esmės šis reguliavimo modelis yra sveikintinas, nes juo užtikrinama tinkama pusiausvyra tarp inovacijų skatinimo ir aukšto lygio aktyvios pagrindinių teisių apsaugos. Tam, kad sistemas būtų galima naudoti konkrečiose aplinkose, pvz., viešųjų paslaugų institucijų arba

ypatingos svarbos infrastruktūros objektų sprendimų priėmimo procesuose, turi būti nustatyti viso pirminio kodo tyrimo būdai.

37. Tačiau EDAV ir EDAPP pasisako už tai, kad pasiūlymo 43 straipsnyje numatyta atitikties vertinimo procedūra būtų pritaikyta tokiu būdu, jog **bendra tvarka būtų numatytas trečiosios šalies atliekamas *ex ante* atitikties vertinimas dėl didelės rizikos DI.** Nors trečiosios šalies atitikties vertinimas dėl didelės rizikos asmens duomenų tvarkymo nėra numatytas BDAR arba ESDAR, DI sistemų keliama rizika dar nėra visiškai suprasta. Todėl įtraukus trečiųjų šalių atitikties vertinimo prievolę bendra tvarka būtų dar labiau padidintas teisinis tikrumas ir pasitikėjimas visomis didelės rizikos DI sistemomis.

2.4.2 Į reguliavimo taikymo sritį taip pat turi būti įtrauktos jau naudojamos DI sistemos

38. Pagal pasiūlymo 43 straipsnio 4 dalį, po reikšmingo pakeitimo didelės rizikos DI sistemoms turėtų būti taikoma nauja atitikties vertinimo procedūra. Teisinga užtikrinti, kad DI sistemos visą jų gyvavimo ciklą atitiktų DI reglamento reikalavimus. DI sistemos, kurios buvo pateiktos rinkai arba pradėtos naudoti prieš pradedant taikyti siūlomą reglamentą (arba po 12 mėnesių, jei tai didelės apimties IT sistema, įtraukta į IX priede pateiktą sąrašą), yra netaikomos, išskyrus atvejus, kai tų sistemų konstrukcija ar paskirtis „reikšmingai pasikeičia“ (83 straipsnis).

39. Vis dėlto „reikšmingų pokyčių“ riba neaiški. Pasiūlymo 66 konstatuojamojoje dalyje nustatyta apatinė pakartotinio atitikties vertinimo riba, „kai įvyksta pokytis, galintis turėti įtakos atitikčiai“. Panaši riba būtų tinkama 83 straipsniui, bent jau didelės rizikos DI sistemoms. Be to, siekiant pašalinti apsaugos spragas, būtina, kad jau sukurtos ir veikiančios DI sistemos (po tam tikro įgyvendinimo etapo) taip pat atitiktų visus DI reglamento reikalavimus.

40. Įvairios asmens duomenų tvarkymo galimybės ir išorės rizika taip pat daro poveikį DI sistemų saugumui. 83 straipsnyje akcentuojami „esminiai konstrukcijos ar numatytos paskirties pakeitimai“ neapima nuorodos į išorės rizikos pokyčius. Todėl į pasiūlymo 83 straipsnį reikėtų įtraukti nuorodą į grėsmės scenarijaus pakeitimus, atsirandančius dėl išorės rizikos, pvz., kibernetinių incidentų, prieštaringų atakų ir pagrįstų vartotojų skundų.

41. Be to, kadangi numatyta, kad reglamentas bus pradėtas taikyti po įsigaliojimo praėjus 24 mėnesiams, EDAPP ir EDAV nemano, kad būtų tikslinga taikyti išimtį dar ilgesnį laikotarpį toms DI sistemoms, kurios jau pateiktos rinkai. Nors pasiūlyme taip pat numatyta, kad vertinant kiekvieną didelės apimties IT sistemą, kaip numatyta IX priede išvardytuose teisės aktuose, atsižvelgiama į reglamento reikalavimus, EDAV ir EDAPP mano, kad DI sistemų naudojimo pradžios reikalavimai turėtų būti taikomi nuo būsimo reglamento taikymo pradžios.

2.5 Valdymas ir Europos DI valdyba

2.5.1 Valdymas

42. EDAV ir EDAPP palankiai vertina tai, kad EDAPP paskirtas atlikti kompetentingos institucijos ir rinkos priežiūros institucijos, atsakingos už Sąjungos institucijų, agentūrų ir įstaigų, patenkančių į šio pasiūlymo taikymo sritį, priežiūrą, funkcijas. EDAPP yra pasirengęs atlikti savo naują ES viešojo administravimo DI reguliuotojo vaidmenį. Tačiau EDAPP funkcijos ir

užduotys nėra išsamiai aprašytos ir turėtų būti plačiau paaiškintos pasiūlyme, ypač kai kalbama apie jo, kaip rinkos priežiūros institucijos, vaidmenį.

43. EDAV ir EDAPP pripažįsta finansinių išteklių paskirstymą, kuris pasiūlyme numatytas Valdybai ir EDAPP, veikiančiam kaip notifikuojančioji įstaiga. Tačiau EDAPP numatytų naujų pareigų vykdymui, neatsižvelgiant į tai, ar jis veikia kaip notifikuotoji įstaiga, reikėtų daug didesnių finansinių ir žmogiškųjų išteklių.

44. Pirma, 63 straipsnio 6 dalies formuluotėje teigiama, kad EDAPP „veikia kaip rinkos priežiūros institucija“ Sąjungos institucijų, agentūrų ir įstaigų, kurios patenka į pasiūlymo taikymo sritį, atžvilgiu, o tai nepaaiškina, ar EDAPP turi būti laikomas visiškai integruota „rinkos priežiūros institucija“, kaip numatyta Reglamente (ES) 2019/1020. Dėl to kyla klausimų dėl EDAPP pareigų ir įgaliojimų praktikoje. Antra, jei į pirmąjį klausimą bus atsakyta teigiamai, neaišku, kaip EDAPP vaidmuo, kaip numatyta ESDAR, gali atitikti Reglamento (ES) 2019/1020 11 straipsnyje numatytą užduotį, kuri apima „veiksmingą internetu tiekiamų gaminių rinkos priežiūrą jų teritorijoje“ arba „fizinius ir laboratorinius patikrinimus remiantis tinkamais pavyzdžiais“. Kyla pavojus, kad naujų užduočių vykdymas be papildomų paaiškinimų pasiūlyme gali kelti pavojų jos, kaip duomenų apsaugos priežiūros institucijos, įsipareigojimų vykdymui.

45. Tačiau EDAV ir EDAPP pabrėžia, kad kai kurios pasiūlymo nuostatos, kuriomis apibrėžiamos įvairių kompetentingų institucijų užduotys ir įgaliojimai pagal DI reglamentą, jų santykiai, pobūdis ir nepriklausomumo garantija, šiuo etapu atrodo neaiškios. Nors Reglamente 2019/1020 teigiama, kad rinkos priežiūros institucija turi būti nepriklausoma, reglamento projekte nereikalaujama, kad priežiūros institucijos būtų nepriklausomos, ir net reikalaujama, kad jos praneštų Komisijai apie tam tikras rinkos priežiūros institucijų, kurios gali būti skirtingos institucijos, atliekamas užduotis. Kadangi pasiūlyme taip pat teigiama, kad duomenų apsaugos institucijos (DAI) vykdys DI sistemų, naudojamų teisėsaugos tikslais, priežiūrą rinkoje (63 straipsnio 5 dalis), tai taip pat reiškia, kad joms, galbūt per savo nacionalinę priežiūros instituciją, bus taikomi ataskaitų teikimo Komisijai įpareigojimai (63 straipsnio 2 dalis), o tai atrodo nesuderinama su jų nepriklausomumu.

46. Todėl EDAV ir EDAPP mano, kad tos nuostatos turi būti patikslintos, suderinant jas su Reglamentu 2019/1020, ESDAR ir BDAR, ir pasiūlyme turėtų būti aiškiai nustatyta, kad priežiūros institucijos pagal DI reglamentą vykdydamos savo užduotis turi būti visiškai nepriklausomos, nes tai būtų esminė garantija siekiant užtikrinti tinkamą būsimo reglamento priežiūrą ir vykdymą.

47. EDAV ir EDAPP primena, kad duomenų apsaugos institucijos jau dabar užtikrina, kad DI sistemoms, susijusioms su asmens duomenimis, būtų taikomas BDAR, ESDAR ir TD siekiant užtikrinti pagrindinių teisių apsaugą ir, tiksliau, teisę į duomenų apsaugą. Todėl duomenų apsaugos institucijos, kaip turėtų būti reikalaujama iš nacionalinių priežiūros institucijų pagal pasiūlymą, jau dabar tam tikru mastu išmano DI technologijas, duomenis ir duomenų skaičiavimą, pagrindines teises, taip pat turi patirties vertinant naujų technologijų keliamą pavojų pagrindinėms teisėms. Be to, kai DI sistemos grindžiamos asmens duomenų tvarkymu arba tvarko asmens duomenis, pasiūlymo nuostatos yra tiesiogiai susijusios su duomenų

apsaugos teisine sistema, o tai bus daugumos DI sistemų, kurioms taikomas šis reglamentas, atveju. Todėl priežiūros institucijų kompetencija pagal pasiūlymą bus susieta su duomenų apsaugos institucijomis.

48. Taigi, jei duomenų apsaugos institucijos būtų paskirtos nacionalinėmis priežiūros institucijomis, būtų užtikrintas labiau suderintas reguliavimo metodas ir prisidėta prie nuoseklesnio duomenų tvarkymo nuostatų aiškinimo ir išvengta prieštaravimų užtikrinant jų vykdymą valstybėse narėse. Be to, visiems DI vertės grandinės suinteresuotiesiems subjektams būtų naudinga turėti bendrą informacinį punktą visoms asmens duomenų tvarkymo operacijoms, patenkančioms į pasiūlymo taikymo sritį, ir apriboti dviejų skirtingų reguliavimo institucijų, kurioms taikomas pasiūlymas ir BDAR, sąveiką. Todėl EDAV ir EDAPP mano, kad **duomenų apsaugos institucijos turėtų būti paskirtos nacionalinėmis priežiūros institucijomis pagal pasiūlymo 59 straipsnį.**

49. Bet kuriuo atveju, kadangi pasiūlyme yra konkrečių taisyklių dėl asmenų apsaugos tvarkant asmens duomenis, priimtų remiantis SESV 16 straipsniu, šių taisyklių laikymąsi, visų pirma apribojimus naudoti DI sistemas nuotoliniam biometriniam tapatybės nustatymui tikruoju laiku viešosiose erdvėse teisėsaugos tikslais, **turi kontroliuoti nepriklausomos institucijos**.

50. Tačiau pasiūlyme nėra aiškios nuostatos, pagal kurią šių taisyklių laikymosi užtikrinimo kompetencija būtų priskirta nepriklausomų institucijų kontrolei. Vienintelė nuoroda į kompetentingas duomenų apsaugos priežiūros institucijas pagal BDAR arba TD yra pasiūlymo 63 straipsnio 5 dalyje, tačiau tik kaip „rinkos priežiūros“ įstaigos arba kartu su kai kuriomis kitomis institucijomis. EDAV ir EDAPP mano, kad ši struktūra neužtikrina SESV 16 straipsnio 2 dalyje ir Chartijos 8 straipsnyje nustatyto nepriklausomos kontrolės reikalavimo laikymosi.

2.5.2 Europos DI valdyba

51. Pasiūlymu įsteigiama Europos dirbtinio intelekto valdyba (EDIV). EDAV ir EDAPP pripažįsta, kad reikia nuosekliai ir suderintai taikyti siūlomą sistemą, taip pat įtraukti nepriklausomus ekspertus į ES DI politikos rengimą. Be to, pasiūlyme numatyta Komisijai suteikti pagrindinį vaidmenį. Iš tiesų ji ne tik priklausytų EDIV, bet ir jai pirmininkautų ir turėtų veto teisę priimant EDIV darbo tvarkos taisykles. Tai prieštarauja poreikiui, kad Europos DI įstaiga būtų nepriklausoma nuo bet kokios politinės įtakos. Todėl EDAV ir EDAPP mano, kad būsimu DI reglamentu **EDIV turėtų būti suteikta daugiau savarankiškumo**, kad ji galėtų iš tikrųjų užtikrinti nuoseklų reglamento taikymą visoje bendrojoje rinkoje.

52. EDAV ir EDAPP taip pat pažymi, kad EDIV nesuteikiama jokių įgaliojimų dėl siūlomo reglamento vykdymo užtikrinimo. Vis dėlto, atsižvelgiant į DI sistemų paplitimą bendrojoje rinkoje ir tarpvalstybinių bylų tikimybę, itin svarbu suderinti vykdymo užtikrinimą ir tinkamai paskirstyti nacionalinių priežiūros institucijų kompetenciją. Todėl EDAV ir EDAPP rekomenduoja būsimame DI reglamente nustatyti nacionalinių priežiūros institucijų bendradarbiavimo mechanizmus. EDAV ir EDAPP siūlo nustatyti mechanizmą, kuriuo būtų užtikrinamas vienas bendras informacinis centras asmenims, kuriems taikomi teisės aktai, ir įmonėms kiekvienos DI sistemos atžvilgiu, ir kad organizacijoms, kurių veikla apima daugiau

nei pusę ES valstybių narių, EDIV galėtų paskirti nacionalinę instituciją, kuri būtų atsakinga už DI reglamento vykdymo užtikrinimą šios DI sistemos atžvilgiu.

53. Be to, atsižvelgiant į nepriklausomą valdybą sudarančių institucijų pobūdį, ji turi teisę veikti savo iniciatyva, o ne tik teikti patarimus ir pagalbą Komisijai. Todėl EDAV ir EDAPP pabrėžia, kad reikia išplėsti Valdybai pavestą misiją, kuri, be kita ko, neatitinka pasiūlyme išvardytų užduočių.

54. Kad šie tikslai būtų pasiekti, **EDIV turi turėti pakankamus ir tinkamus įgaliojimus**, o jos teisinis statusas turėtų būti patikslintas. Visų pirma tam, kad būsimo reglamento materialinė taikymo sritis išliktų aktuali, į jo raidą būtina įtraukti už jo taikymą atsakingas institucijas. Todėl EDAV ir EDAPP rekomenduoja, kad EDIV būtų suteikti įgaliojimai siūlyti Komisijai I priedo, kuriame apibrėžiamos DI priemonės ir metodai, ir III priedo, kuriame išvardijamos 6 straipsnio 2 dalyje nurodytos didelės rizikos DI sistemos, pakeitimus. Komisija taip pat turėtų konsultuotis su EDIV prieš bet kokius šių priedų pakeitimus.

55. Pasiūlymo 57 straipsnio 4 dalyje numatyta, kad Valdyba keičiasi informacija su kitais Sąjungos organais, tarnybomis, agentūromis ir patariamosiomis grupėmis. Atsižvelgdami į savo ankstesnį darbą DI srityje ir savo ekspertines žinias žmogaus teisių srityje, EDAV ir EDAPP rekomenduoja Pagrindinių teisių agentūrą laikyti viena iš Valdybos stebėtojų.

3 SĄVEIKA SU DUOMENŲ APSAUGOS SISTEMA

3.1 Pasiūlymo ryšys su galiojančiais ES duomenų apsaugos teisės aktais

56. Aiškiai apibrėžtas pasiūlymo ir galiojančių duomenų apsaugos teisės aktų ryšys yra būtina išankstinė sąlyga siekiant užtikrinti, kad būtų laikomasi ES *acquis* asmens duomenų apsaugos srityje ir kad jis būtų taikomas. Tokie ES teisės aktai, t. y. BDAR, ESDAR ir TD, turi būti laikomi privalomais ir jais turi būti grindžiami tolesni pasiūlymai dėl teisėkūros procedūra priimamų aktų, nedarant poveikio esamoms nuostatoms ir nekeičiant jų, įskaitant ir tuos atvejus, kai tai yra priežiūros ir valdymo institucijų kompetencijų ribose.

57. Todėl, EDAV ir EDAPP nuomone, svarbu pasiūlyme aiškiai vengti bet kokio nesuderinamumo ir galimo prieštaravimo su BDAR, ESDAR ir TD. Tai daroma ne tik siekiant teisinio tikrumo, bet ir siekiant išvengti tiesioginės ar netiesioginės pasiūlymo keliamos grėsmės pagrindinei teisei į asmens duomenų apsaugą, įtvirtintai SESV 16 straipsniu ir Chartijos 8 straipsniu.

58. Visų pirma, savarankiškai besimokančios mašinos galėtų apsaugoti asmenų asmens duomenis tik tuo atveju, jei tai būtų įdiegta tikslingai. Taip pat labai svarbu suteikti galimybę asmenims naudotis savo teisėmis pagal BDAR 22 straipsnį (automatinis individualių sprendimų priėmimas, įskaitant profiliavimą) arba ESDAR 23 straipsnį nedelsiant, nepriklausomai nuo duomenų tvarkymo tikslų. Šiuo atžvilgiu DI sistemose turi būti nuo pat pradžių numatytos kitos duomenų subjektų teisės, susijusios su teise ištrinti ar ištaisyti duomenis pagal duomenų apsaugos teisės aktus, nepriklausomai nuo pasirinkto DI metodo ar techninės architektūros.

59. Naudojant asmens duomenis DI sistemų mokymui DI sistemų pagrindinėse dalyse gali atsirasti šališkų sprendimų priėmimo modelių. Todėl įvairios apsaugos priemonės yra būtinos šiuose procesuose, visų pirma, kvalifikuota žmogaus priežiūra, kad duomenų subjektų teisės būtų gerbiamos ir užtikrinta jų apsauga, taip pat siekiant išvengti bet kokio neigiamo poveikio asmenims. Kompetentingoms institucijoms taip pat turėtų būti suteikta galimybė siūlyti DI sistemų šališkumo vertinimo gaires ir padėti vykdyti žmogaus vykdomą priežiūrą.

60. Duomenų subjektai visada turėtų būti informuojami, kada jų duomenys naudojami DI mokymui ir (arba) prognozavimui, apie tokio tvarkymo teisinį pagrindą, bendrą DI sistemos logikos (procedūros) ir taikymo srities paaiškinimą. Šiuo atžvilgiu tokiais atvejais visada turėtų būti užtikrinta fizinių asmenų teisė riboti duomenų tvarkymą (BDAR 18 straipsnis ir ESDAR 20 straipsnis), taip pat pašalinti ir (arba) ištrinti duomenis (BDAR 16 straipsnis ir ESDAR 19 straipsnis). Be to, duomenų valdytojas turėtų būti aiškiai įpareigotas informuoti duomenų subjektą apie duomenų ginčijimui, ribojimui, pašalinimui ir pan. taikomus laikotarpius. DI sistema turi atitikti visus duomenų apsaugos reikalavimus taikant tinkamas technines ir organizacines priemones. Teisė į paaiškinimą turėtų užtikrinti papildomą skaidrumą.

3.2 Bandomoji aplinka ir tolesnis duomenų tvarkymas (pasiūlymo 53 ir 54 straipsniai)

61. Atsižvelgiant į esamus teisinius ir moralinius apribojimus, svarbu skatinti Europos inovacijas naudojant tokias priemones kaip bandomoji aplinka. Bandomoji aplinka suteikia galimybę nustatyti apsaugos priemones, kurių reikia siekiant didinti pasitikėjimą DI sistemomis ir jomis pasikliauti. Sudėtingoje aplinkoje dirbtinio intelekto specialistams gali būti sunku tinkamai įvertinti visus interesus. Ypač ribotus išteklius turinčios mažosios ir vidutinės įmonės, veikiančios apribotoje bandomojoje reglamentavimo aplinkoje, gali greičiau pateikti įžvalgas ir taip paskatinti inovacijas.

62. Pasiūlymo 53 straipsnio 3 dalyje teigiama, kad bandomoji aplinka nedaro poveikio priežiūros ir korekcinėms priemonėms. Jei šis paaiškinimas yra naudingas, taip pat reikia parengti nurodymus arba gaires, kaip užtikrinti tinkamą pusiausvyrą tarp priežiūros institucijos statuso ir išsamių rekomendacijų teikimo bandomojoje aplinkoje.

63. 53 straipsnio 6 skirsnyje aprašyta, kad bandomosios aplinkos naudojimo būdas ir sąlygos nustatomos įgyvendinimo aktuose. Svarbu parengti specialias gaires, kad būtų užtikrintas nuoseklumas ir parama kuriant ir eksploatuojant bandomąsias aplinkas. Tačiau privalomais įgyvendinimo aktais galėtų būti ribojamos kiekvienos valstybės narės galimybės pritaikyti bandomąją aplinką pagal savo poreikius ir vietos praktiką. Todėl EDAV ir EDAPP rekomenduoja, kad EDIV geriau vietoj to pateiktų gaires dėl bandomųjų aplinkų.

64. Pasiūlymo 54 straipsniu siekiama suteikti teisinį pagrindą tolesniam asmens duomenų tvarkymui kuriant tam tikras DI sistemas viešojo intereso tikslais apribotoje bandomojoje DI reglamentavimo aplinkoje. Pasiūlymo 54 straipsnio 1 dalies ryšys su pasiūlymo 54 straipsnio 2 dalimi ir 41 konstatuojamąja dalimi, taigi ir su galiojančiais ES duomenų apsaugos teisės aktais, tebėra neaiškus. Tačiau BDAR ir ESDAR jau nustatytas tolesnio duomenų tvarkymo pagrindas. Ypač tais atvejais, kai tolesnis duomenų tvarkymas atitinka viešąjį interesą; duomenų valdytojo interesų ir duomenų subjekto interesų derinimas neturi stabdyti inovacijų.

Pasiūlymo 54 straipsnyje šiuo metu nenagrinėjami du svarbūs klausimai: i) kokiomis aplinkybėmis, naudojant (papildomus) kriterijus, įvertinami duomenų subjektų interesai ir ii) ar šios DI sistemos bus naudojamos tik bandomojoje aplinkoje. EDAV ir EDAPP palankiai vertina reikalavimą dėl Sąjungos arba valstybės narės teisės akto, kai pagal TD surinkti asmens duomenys tvarkomi bandomojoje aplinkoje, tačiau rekomenduoja konkrečiau patikslinti, kas numatoma – vadovaujantis BDAR ir ESDAR, turi būti paaiškinta, kad tokių bandomųjų aplinkų teisinis pagrindas turėtų atitikti BDAR 23 straipsnio 2 dalyje ir ESDAR 25 straipsnyje nustatytus reikalavimus, – ir nurodo, kad kiekvienas bandomosios aplinkos naudojimo atvejis turi būti nuodugniai įvertintas. Tai taip pat taikoma visam 54 straipsnio 1 dalies b–j punktuose nurodytų sąlygų sąrašui.

65. Kai kurie pasiūlymo 54 straipsnyje pateikti papildomi argumentai dėl pakartotinio duomenų naudojimo rodo, kad naudojant bandomąją aplinką reikia daug išteklių ir todėl realu teigti, kad tik nedaugeliui įmonių būtų suteikta galimybė dalyvauti. Dalyvavimas bandomojoje aplinkoje galėtų teikti konkurencinį pranašumą. Norint pakartotinai naudoti duomenis, reikėtų atidžiai apsvarstyti, kaip atrinkti dalyvius, siekiant užtikrinti, kad jie patektų į taikymo sritį, ir išvengiant neteisingo vertinimo. EDAV ir EDAPP susirūpinimą kelia tai, kad suteikus galimybę pakartotinai naudoti duomenis bandomojoje aplinkoje nukrypstama nuo BDAR nustatyto atskaitomybės metodo, pagal kurį atsakomybė tenka duomenų valdytojui, o ne kompetentingai institucijai.

66. Be to, EDAV ir EDAPP mano, kad, atsižvelgiant į bandomosios aplinkos tikslus, t. y. kurti, bandyti ir tvirtinti DI sistemas, bandomoji aplinka negali patekti į TD taikymo sritį. Nors TD numatytas pakartotinis duomenų naudojimas moksliniams tyrimams, tuo antriniu tikslu tvarkomiems duomenims bus taikomas BDAR arba ESDAR, o nebe TD.

67. Ką apims apribota bandomoji reglamentavimo aplinka yra neaišku. Kyla klausimas, ar į siūlomą apribotą bandomąją reglamentavimo aplinką įtraukta kiekvienoje valstybėje narėje esanti IT infrastruktūra, numatant tam tikrus papildomus teisinius pagrindus tolesniam tvarkymui, ar tik suteikiama galimybė naudotis reguliavimo praktine patirtimi ir gairėmis. EDAV ir EDAPP ragina teisės aktų leidėją paaiškinti šią sampratą pasiūlyme ir aiškiai jame nurodyti, kad apribota bandomoji reglamentavimo aplinka neįpareigoja kompetentingų institucijų teikti savo techninę infrastruktūrą. Bet kuriuo atveju pagal tokius išaiškinimus kompetentingoms institucijoms turi būti suteikiami atitinkami finansiniai ir žmogiškieji ištekliai.

68. Galiausiai EDAV ir EDAPP norėtų pabrėžti tarpvalstybinių DI sistemų, kurios bus prieinamos visai Europos bendrajai skaitmeninei rinkai, plėtojimą. Tokiais DI sistemų atvejais apribota bandomoji reglamentavimo aplinka, kaip inovacijų priemonė, neturėtų tapti kliūtimi tarpvalstybinei plėtrai. Todėl EDAV ir EDAPP rekomenduoja taikyti koordinuotą tarpvalstybinį požiūrį, kuris vis dar yra pakankamai prieinamas nacionaliniu lygmeniu visoms MVĮ, ir siūlo bendrą sistemą visoje Europoje, kuri nebūtų pernelyg ribojanti. Būtina užtikrinti Europos koordinavimo ir nacionalinių procedūrų pusiausvyrą ir išvengti prieštaringo būsimo DI reglamento, kuris trukdytų diegti inovacijas visoje ES, įgyvendinimo.

3.3 Skaidrumas

69. EDAV ir EDAPP palankiai vertina reikalavimą registruoti didelės rizikos DI sistemas viešoje duomenų bazėje (kaip nurodyta pasiūlymo 51 ir 60 straipsniuose). Ši duomenų bazė turėtų sudaryti sąlygas teikti plačiajai visuomenei informaciją apie DI sistemos taikymo sritį ir žinomus trūkumus bei incidentus, kurie galėtų kelti pavojų jos veikimui, ir apie priemones, kurias paslaugų teikėjai taiko siekdami juos pašalinti ir ištaisyti.

70. Pagrindinis demokratinis principas – tai stabdžių ir atsvarų sistema. Todėl tai, kad skaidrumo pareiga netaikoma DI sistemoms, naudojamoms nusikalstamoms veikoms nustatyti, užkardyti, tirti ar patraukti baudžiamojon atsakomybėn už jas, yra pernelyg plati išimtis. Reikia atskirti DI sistemas, kurios naudojamos aptikti arba užkirsti kelią, ir DI sistemas, kuriomis siekiama atlikti tyrimą siekiant padėti patraukti baudžiamojon atsakomybėn už nusikalstamas veikas. Prevencijos ir aptikimo apsaugos priemonės turi būti griežtesnės dėl nekaltumo prezumpcijos. Be to, EDAV ir EDAPP apgailestauja, kad pasiūlyme nėra įspėjimų dėl atsargumo, o tai gali būti suprantama kaip „žalia šviesa“ naudojant net ir nepatikrintas didelės rizikos DI sistemas ar taikomąsias programas.

71. Tais atvejais, kai dėl slaptumo net ir gerai veikiančioje demokratijoje skaidrumas visuomenės atžvilgiu yra ribotas ar visai neįmanomas, turėtų būti nustatytos apsaugos priemonės, taip pat tokios DI sistemos turėtų būti registruojamos kompetentingų priežiūros institucijų ir užtikrinamas skaidrumas šių institucijų atžvilgiu.

72. DI sistemų skaidrumo užtikrinimas yra labai sudėtingas uždavinys. Visiškai kiekybinis daugelio DI sistemų sprendimų priėmimo metodas, kuris iš esmės skiriasi nuo žmogiškojo požiūrio, kuris daugiausia grindžiamas priežastiniu ir teoriniu argumentavimu, gali prieštarauti poreikiui gauti iš anksto suprantamą mašinų rezultatų paaiškinimą. Reglamentu turėtų būti skatinami nauji, aktyvesni ir laiku įgyvendinami būdai informuoti DI sistemų naudotojus apie (sprendimų priėmimo) statusą sistemoje bet kuriuo metu, iš anksto įspėjant apie galimus žalingus rezultatus, kad asmenys, kurių teises ir laisves mašinų savarankiški sprendimai gali pažeisti, galėtų reaguoti arba ginčyti sprendimą.

3.4 Specialių kategorijų duomenų tvarkymas; su nusikalstamomis veikomis susiję duomenys

73. Specialių kategorijų duomenų tvarkymas teisėsaugos srityje reglamentuojamas pagal ES duomenų apsaugos sistemos nuostatas, įskaitant TD, taip pat jos įgyvendinimą nacionaliniu lygmeniu. Pasiūlyme reikalaujama nesuteikti bendro teisinio pagrindo tvarkyti asmens duomenis, įskaitant specialių kategorijų asmens duomenis, plg. 41 konstatuojamąją dalį. Kartu pasiūlymo 10 straipsnio 5 dalyje nurodoma, kad „tokių sistemų teikėjai gali tvarkyti specialių kategorijų asmens duomenis“. Be to, pagal tą pačią nuostatą reikalaujama papildomų apsaugos priemonių, taip pat pateikiant pavyzdžių. Todėl atrodo, kad pasiūlymas trukdo taikyti BDAR, TD ir ESDAR. Nors EDAV ir EDAPP palankiai vertina pastangas nustatyti tinkamas apsaugos priemones, reikalingas nuoseklesnis reguliavimo metodas, nes dabartinės nuostatos neatrodo pakankamai aiškios, kad būtų sukurtas specialių kategorijų duomenų tvarkymo teisinis pagrindas, ir jas reikia papildyti papildomomis apsaugos priemonėmis, kurias dar reikia įvertinti. Be to, kai asmens

duomenys renkami tvarkant duomenis pagal TD, reikės atsižvelgti į galimas papildomas apsaugos priemones ir apribojimus, susijusius su TD perkėlimu į nacionalinę teisę.

3.5 Atitikties užtikrinimo mechanizmai

3.5.1 Sertifikavimas

74. Vienas iš pagrindinių pasiūlymo ramsčių yra sertifikavimas. Pasiūlyme išdėstyta sertifikavimo sistema grindžiama subjektų struktūra (notifikuojančiosios institucijos / notifikuotosios įstaigos / Komisija) ir atitikties vertinimo / sertifikavimo mechanizmu, apimančiu privalomus reikalavimus, taikomus didelės rizikos DI sistemoms, ir grindžiama Europos darniaisiais standartais pagal Reglamentą (ES) Nr. 1025/2012 ir bendromis specifikacijomis, kurias turi nustatyti Komisija. Šis mechanizmas skiriasi nuo sertifikavimo sistemos, kuria siekiama užtikrinti duomenų apsaugos taisyklių ir principų laikymąsi, kaip nurodyta BDAR 42 ir 43 straipsniuose. Tačiau neaišku, kaip notifikuotųjų įstaigų pagal pasiūlymą išduoti sertifikatai gali būti susieti su BDAR numatytais duomenų apsaugos sertifikatais, ženklais ir žymenimis kitaip nei tai, kas numatyta kitų tipų sertifikatams (žr. 42 straipsnio 2 dalį dėl sertifikatų, kurie išduodami pagal Reglamentą (ES) 2019/881).

75. Kadangi didelės rizikos DI sistemos grindžiamos asmens duomenų tvarkymu arba jose asmens duomenys tvarkomi tam, kad jos atliktų numatytą užduotį, dėl šių neatitikimų visoms susijusioms įstaigoms gali kilti teisinis netikrumas, nes dėl jų gali susidaryti situacijų, kai pagal pasiūlymą sertifikuotos ir CE atitikties ženklu pažymėtos DI sistemos, pateiktos rinkai arba pradėtos naudoti, gali būti naudojamos nesilaikant duomenų apsaugos taisyklių ir principų.

76. Pasiūlyme trūksta aiškaus ryšio su duomenų apsaugos teise, taip pat su kitais ES ir valstybių narių teisės aktais, taikytinais kiekvienai III priede nurodytai didelės rizikos DI sistemos sričiai. Visų pirma į pasiūlymą reikėtų įtraukti duomenų kiekio mažinimo ir pritaikytosios duomenų apsaugos principus kaip vieną iš aspektų, į kurį reikia atsižvelgti prieš gaunant CE ženklą, dėl galimai didelio DI sistemų poveikio pagrindinėms privatumo ir asmens duomenų apsaugos teisėms ir poreikio užtikrinti aukštą pasitikėjimo DI sistema lygį. Todėl EDAV ir EDAPP rekomenduoja iš dalies keisti pasiūlymą, kad būtų paaiškintas pagal minėtą reglamentą išduotų sertifikatų ir duomenų apsaugos sertifikatų, ženklų ir žymenų santykis. Galiausiai duomenų apsaugos institucijos turėtų dalyvauti rengiant ir nustatant darniuosius standartus ir bendrąsias specifikacijas.

77. Atsižvelgiant į pasiūlymo 43 straipsnį, susijusį su atitikties vertinimu, 47 straipsnyje nustatyta nuo atitikties vertinimo procedūros leidžianti nukrypti nuostata atrodo labai plati, įtraukianti pernelyg daug išimčių, pavyzdžiui, dėl išskirtinių priežasčių, susijusių su visuomenės saugumu arba žmonių gyvybės ir sveikatos apsauga, aplinkos apsauga ir pagrindinio pramoninio ir infrastruktūros turto apsauga. Siūlytume teisės aktų leidėjams jas susiaurinti.

3.5.2 Elgesio kodeksai

78. Pagal pasiūlymo 69 straipsnį Komisija ir valstybės narės skatina ir padeda rengti elgesio kodeksus, kuriais siekiama, kad nedidelės rizikos DI sistemų teikėjai savanoriškai taikytų didelės rizikos DI sistemoms taikomus reikalavimus, taip pat papildomus reikalavimus. Pagal BDAR 78 konstatuojamąją dalį EDAV ir EDAPP rekomenduoja nustatyti ir apibrėžti šių priemonių ir BDAR numatytų Elgesio kodekso nuostatų, kuriomis padedama laikytis duomenų apsaugos reikalavimų, sąveiką. Atsižvelgiant į tai, svarbu paaiškinti, ar asmens duomenų apsauga turi būti laikoma vienu iš „papildomų reikalavimų“, kuriuos gali spręsti 69 straipsnio 2 dalyje nurodytos Elgesio kodekso nuostatos. Taip pat svarbu užtikrinti, kad „techninės specifikacijos ir sprendimai“, kuriuos nagrinėja 69 straipsnio 1 dalyje nurodytos Elgesio kodekso nuostatos, skirtos skatinti laikytis DI reglamento projekto reikalavimų, neprieštarautų BDAR ir ESDAR taisyklėms ir principams. Todėl būtų naudinga, kad nedidelės rizikos DI sistemų teikėjai taikytų šias priemones, jei tokios sistemos būtų grindžiamos asmens duomenų tvarkymu arba asmens duomenys tvarkomi, siekiant atlikti numatytą užduotį, nes taip būtų užtikrinta, kad duomenų valdytojai ir tvarkytojai, naudodamiesi šiomis sistemomis, galėtų vykdyti savo duomenų apsaugos prievoles.

79. Be to, patikimo dirbtinio intelekto teisinę sistemą papildytų Elgesio kodekso integravimas, taip didinant pasitikėjimą, kad ši technologija naudojama saugiu būdu ir laikantis teisės aktų, įskaitant pagarbą pagrindinėms teisėms. Tačiau kuriant šias priemones, reikėtų numatyti būdus, kaip patikrinti, ar tokiuose kodeksuose numatytos veiksmingos „techninės specifikacijos ir sprendimai“, ir į atitinkamų kodeksų dalis įtraukti „aiškius tikslus ir pagrindinius veiklos rodiklius, kuriais matuojamas tikslų siekimas“. Be to, kai nėra jokios nuorodos į (privalomus) elgesio kodeksų stebėsenos mechanizmus, kuriais būtų patikrinama, ar nedidelės rizikos DI sistemų teikėjai laikosi jų nuostatų, ir atskirų teikėjų galimybės parengti (ir patiems įgyvendinti) minėtus kodeksus (žr. aiškinamojo memorandumo 5.2.7 skirsnį), gali sumažėti šių priemonių veiksmingumas ir galimybės jas įgyvendinti.

80. Galiausiai EDAV ir EDAPP prašo paaiškinti, kokių rūšių iniciatyvas Komisija gali parengti pagal pasiūlymo 81 konstatuojamąją dalį, „kad būtų lengviau mažinti technines kliūtis, trukdančias keistis duomenimis tarpvalstybiniu mastu DI plėtojimo tikslais“.

4 IŠVADA

81. Nors EDAV ir EDAPP palankiai vertina Komisijos pasiūlymą ir mano, kad toks reglamentas yra būtinas siekiant užtikrinti ES piliečių ir gyventojų pagrindines teises, jie mano, kad siekiant užtikrinti pasiūlymo taikymą ir veiksmingumą, jį reikia pritaikyti keliais aspektais.

82. Atsižvelgiant į pasiūlymo sudėtingumą ir spręstinus klausimus, dar reikia daug nuveikti, kol pasiūlymu bus sukurta gerai veikianti teisinė sistema, veiksmingai papildanti BDAR pagrindinių žmogaus teisių apsaugos srityje, kartu skatinant inovacijas. EDAV ir EDAPP ir toliau galės pasiūlyti savo paramą šiame procese.

2021 m. birželio 18 d., Briuselis

Europos duomenų apsaugos valdybos vardu	Europos duomenų apsaugos priežiūros pareigūno vardu
Pirmininkė	Priežiūros pareigūnas
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI