



Briuselis, 2020 02 19
COM(2020) 65 final

BALTOJI KNYGA

Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą

Baltoji knyga „Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“

Dirbtinis intelektas (DI) sparčiai tobulėja. Jis pakeis mūsų gyvenimą, padėdamas užtikrinti geresnę sveikatos priežiūrą (pvz., tikslesnį diagnozavimą ir geresnę ligų prevenciją), efektyviau ūkininkauti, švelninti klimato kaitą ir prisitaikyti prie jos, didinti gamybos sistemų veiksmingumą dėl prognozuojamosios priežiūros, didinti europiečių saugumą ir įvairiais kitais būdais, kuriuos kol kas menkai įsivaizduojame. Kartu DI gali atnešti nemažai pavojų, tokių kaip neskaidrus sprendimų priėmimas, diskriminacija dėl lyties arba kitų veiksnių, brovimasis į privačią erdvę arba naudojimas nusikalstamais tikslais.

Nuožnios pasaulinės konkurencijos sąlygomis reikalingas tvirtas europinis požiūris, grindžiamas 2018 m. balandžio mėn. pristatyta Europos dirbtinio intelekto strategija¹. Norėdama išnaudoti DI teikiamas galimybes ir atremti dėl jo kylančius iššūkius, ES turi veikti vieningai, kaip kumštis, ir remdamasi Europos vertybėmis rasti savo būdą, kaip plėtoti ir diegti DI.

Komisija yra įsipareigojusi sudaryti sąlygas mokslo proveržiui, išsaugoti ES technologinę lyderystę ir užtikrinti, kad naujos technologijos neštų naudą visiems europiečiams – jų gyvenimas gerėtų, o teisės nebūtų pažeidžiamos.

Komisijos Pirmininkė Ursula von der Leyen savo politinėse gairėse² paminėjo suderintą Europos požiūrį į DI poveikį žmogui ir etikai, taip pat svarstymus dėl geresnio didžiųjų duomenų naudojimo inovacijoms kurti.

Todėl Komisija palaiko į reglamentavimą ir investicijas orientuotą požiūrį siekiant dvejopo tikslo – skatinti plačiau diegti DI ir mažinti riziką, susijusią su tam tikrais šios naujos technologijos naudojimo būdais. Šios baltosios knygos tikslas – išnagrinėti politikos galimybes, kaip pasiekti šiuos tikslus. Joje neaptariami DI plėtojimo ir naudojimo karinėms reikmėms klausimai. Komisija ragina valstybes nares, kitas Europos institucijas ir visus suinteresuotuosius subjektus, įskaitant pramonės subjektus, socialinius partnerius, pilietinės visuomenės organizacijas, mokslininkus, plačiąją visuomenę ir visas suinteresuotąsias šalis, išsakyti savo nuomonę apie toliau aptariamas galimybes ir taip padėti Komisijai priimti šios srities sprendimus ateityje.

1. ĮVADAS

Kadangi skaitmeninės technologijos tampa vis svarbesnės visoms žmogaus gyvenimo sferoms, žmogus turėtų galėti jomis pasitikėti. Tad patikimumas yra būtina jų naudojimo sąlyga. Tai galimybė Europai, kuri puoselėja vertybes, tvirtai remia teisinės valstybės principą ir yra įrodžiusi, jog geba kurti saugius, patikimus ir sudėtingus įvairių sričių – nuo aeronautikos iki energetikos, automobilių ir medicinos įrangos – produktus ir paslaugas.

Tvarus Europos ekonomikos augimas ir visuomenės gerovė vis labiau priklauso ir priklausys nuo duomenų sukuriamos vertės. DI yra viena iš svarbiausių duomenų ekonomikos technologijų. Šiandien dauguma duomenų yra susiję su vartotojais ir laikomi bei tvarkomi centrinėje debesijos infrastruktūroje. Ateityje, priešingai, didelė dalis kur kas gausesnių duomenų bus sukuriamą pramonės, verslo ir viešajame sektoriuose ir jie bus laikomi įvairiose sistemose, visų pirma tinklo paribyje

¹ Dirbtinis intelektas Europai, COM(2018) 237 final.

² https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_lt.pdf.

veikiančiuose kompiuteriniuose prietaisuose. Tai atveria naujų galimybių Europai, kurios pozicijos skaitmeninės pramonės ir verslo (B2B) prietaikų srityje yra tvirtos, tačiau palyginti silpnos vartotojų platformų srityje.

Paprastaiariant, DI yra technologijos, kurias taikant derinami duomenys, algoritmai ir kompiuterijos pajėgumai. Todėl kompiuterijos pažanga ir didėjantis duomenų prieinamumas yra pagrindiniai veiksniai, lemiantys dabartinį DI pakilimą. Europa gali pasinaudoti savo technologijų ir pramonės pranašumais kartu su kokybiška skaitmenine infrastruktūra ir pagrindinėmis vertybėmis grindžiama reguliavimo sistema, kad **taptų pasauline duomenų ekonomikos ir jos prietaikų inovacijų lydere**, kaip nustatyta Europos duomenų strategijoje³. Tuo remdamasi ji gali sukurti DI ekosistemą, kurios technologijos būtų naudingos visai Europos visuomenei ir ekonomikai:

- nauja nauda **piliečiams**, pavyzdžiui, geresnė sveikatos priežiūra, mažiau gendantį buitįs įrangą, saugesnio ir švaresnio transporto sistemos, geresnės viešosios paslaugos,
- plėtos galimybės **verslui**, pavyzdžiui, naujos kartos produktai ir paslaugos tose srityse, kuriose Europa yra ypač stipri (mašinos, transportas, kibernetinis saugumas, ūkininkavimas, žaliųjų ir žiedinė ekonomika, sveikatos priežiūra ir didelės pridėtinės vertės sektoriai, pvz., mada ir turizmas), ir
- **viešojo intereso** paslaugas teikiantiems subjektams, pavyzdžiui, mažesnė (transporto, švietimo, energetikos ir atliekų tvarkymo) paslaugų teikimo kaina, didesnis produktų tvarumas⁴ ir tinkamos priemonės teisėsaugos institucijoms⁵ piliečių saugumui užtikrinti, kartu taikant tinkamas priemones jų teisėms ir laisvėms apsaugoti.

Atsižvelgiant į didelį galimą DI poveikį mūsų visuomenei ir poreikį stiprinti pasitikėjimą, labai svarbu, kad Europoje DI būtų grindžiamas mūsų vertybėmis ir pagrindinėmis teisėmis, tokiomis kaip žmogaus orumas ir privatumo apsauga.

Be to, reikėtų apgalvoti ne tik tai, kaip DI sistemos paveiks atskirus asmenis, bet ir kokį poveikį jos padarys visai visuomenei. DI sistemų naudojimas gali būti reikšmingas siekiant darnaus vystymosi tikslų, palaikant demokratiją ir užtikrinant socialines teises. Naujaisiais Europos žaliojo kurso pasiūlymais⁶ Europa rodo kelią, kaip spręsti su klimatu ir aplinka susijusias problemas. Labai svarbi varomoji jėga siekiant žaliojo kurso tikslų yra tokios skaitmeninės technologijos kaip DI. Atsižvelgiant į didėjančią DI svarbą, reikia deramai apsvarstyti DI sistemų poveikį aplinkai per visą jų gyvavimo ciklą ir visoje tiekimo grandinėje, pvz., tai, kiek išteklių sunaudojama algoritmams mokytis ir duomenims saugoti.

Bendras Europos požiūris į DI yra būtinasis, kad būtų pasiektas pakankamas mastas ir išvengta bendrosios rinkos susiskaidymo. Apsiribojant nacionalinėmis iniciatyvomis, gali kilti pavojus teisiniam tikrumui, silpnėti piliečių pasitikėjimas ir rasti kliūčių dinamiškos Europos pramonės formavimuisi.

³ COM(2020) 66 *final*.

⁴ DI ir skaitmeninimas apskritai yra itin svarbūs veiksniai siekiant Europos žaliojo kurso tikslų. Tačiau apskaičiuota, kad dabar IRT sektoriui tenka daugiau kaip 2 proc. viso pasaulyje išmetamo anglies dioksido kiekio. Kartu su šia baltąja knyga skelbiamoje Europos skaitmeninėje strategijoje siūlomos žaliosios pertvarkos priemonės skaitmeninių technologijų sektoriui.

⁵ DI priemonės gali padėti geriau apsaugoti ES piliečius nuo nusikaltimų ir teroro aktų. Pavyzdžiui, jos galėtų padėti atpažinti terorizmo propagandą internete, nustatyti įtartinus pavojingų produktų pardavimo sandorius, aptikti pavojingus slepiamus daiktus, neteisėtas medžiagas ar produktus, teikti pagalbą piliečiams ekstremaliosiose situacijose ir susiorientuoti pirmojo reagavimo pajėgoms.

⁶ COM(2019) 640 *final*.

Šioje baltojoje knygoje pristatomos politikos galimybės, kuriomis sudaromos sąlygos DI Europoje plėtoti patikimai ir saugiai, visapusiškai atsižvelgiant į ES piliečių vertybes ir teises. Šią baltąją knygą sudaro:

- politikos strategija dėl priemonių Europos, nacionalinio ir regioninio lygmenų pastangoms suderinti. Bendradarbiaujant privačiajam ir viešajam sektoriams strategija siekiama sutelkti išteklius sukurti **kompetencijos ekosistemi**, apimančiai visą vertės grandinę, pradedant nuo mokslinių tyrimų ir inovacijų, ir pasiūlyti tinkamų paskatų, be kita ko, mažosioms ir vidutinėms įmonėms (MVI), sparčiau apsispręsti naudoti DI sprendimus;
- pagrindiniai būsimos Europos DI reglamentavimo sistemos, sukursiančios unikalią **pasitikėjimo ekosistemą**, elementai. Tam reikia užtikrinti, kad būtų laikomasi ES taisyklių, įskaitant pagrindinių teisių ir vartotojų teisių apsaugos taisykles, ir visų pirma kad jas atitiktų ES naudojamos DI sistemos, kurios kelia didelę riziką⁷. Sukurti pasitikėjimo ekosistemą yra politikos uždavinys ir tai turėtų padidinti piliečius naudoti AI prietaikus, o įmonėms ir viešosioms organizacijoms suteikti teisinį tikrumą kurti inovacijas naudojant DI. Komisija tvirtai palaiko orientavimąsi į žmogų, remdamasi komunikatu „Pasitikėjimo į žmogų orientuotu dirbtiniu intelektu didinimas“⁸, taip pat atsižvelgs į Aukšto lygio ekspertų grupės dirbtinio intelekto klausimais parengtų Etikos gairių taikymo bandomajame etape gautą informaciją.

Kartu su šia baltąja knyga skelbiamos Europos duomenų strategijos tikslas – sudaryti sąlygas Europai tapti patraukliausia, saugiausia ir dinamiškiausia duomenų ekonomika pasaulyje, kad duomenys suteiktų Europai galių priimti geresnius sprendimus ir pagerinti visų savo piliečių gyvenimą. Šiam tikslui pasiekti strategijoje nustatytos kelios politikos priemonės, be kita ko, privačiųjų ir viešųjų investicijų telkimas. Be to, kartu su šia baltąja knyga skelbiamoje Komisijos ataskaitoje analizuojamas poreikis DI, daiktų internetą ir kitas skaitmenines technologijas įtraukti į teisės aktus, kuriais reglamentuojama sauga ir civilinė atsakomybė.

2. PRAMONĖS IR PROFESINIŲ RINKŲ PRANAŠUMŲ IŠNAUDOJIMAS

Europa turi geras galimybes pasinaudoti DI potencialu ne tik naudodama šią technologiją, bet ir ją kurdama bei gamindama. Joje yra puikių mokslinių tyrimų centrų, novatoriškų startuolių, pasaulyje ji pirmauja robotikos ir konkurencinguose gamybos ir paslaugų sektoriuose – nuo automobilių gamybos iki sveikatos priežiūros, energetikos, finansinių paslaugų ir žemės ūkio. Europa yra sukūrusi puikią kompiuterijos infrastruktūrą (pvz., turi našųjų kompiuterių), be kurios DI veikimas būtų neįmanomas. Europa taip pat turi daugybę viešųjų ir pramonės duomenų, kurių potencialas šiuo metu išnaudojamas nepakankamai. Ji turi pripažintų pramonės pranašumų kuriant saugias ir patikimas mažos vartojamosios galios skaitmenines sistemas, kurios yra būtinos tolesnei DI plėtočiai.

Pasinaudojus ES pajėgumais investuoti į naujos kartos technologijas ir infrastruktūrą, taip pat į skaitmeninius gebėjimus, pvz., gebėjimą naudotis duomenimis, padidės Europos technologinis suverenumas duomenų ekonomikai svarbių bazinių didelio poveikio technologijų ir infrastruktūros srityse. Infrastruktūra turėtų padėti kurti Europos duomenynus, sudarančius sąlygas patikimam, t. y. Europos vertybėmis ir taisyklėmis grindžiamam, DI.

⁷ Nors siekiant užkirsti kelią DI naudojimui nusikalstamiems tikslams ir su tuo kovoti gali prireikti papildomų priemonių, jos šioje baltojoje knygoje neapartiamos.

⁸ COM(2019) 168.

Europa turėtų pasinaudoti savo stiprybėmis, kad sustiprintų savo pozicijas ekosistemose ir visoje vertės grandinėje, nuo tam tikrų aparatinės įrangos gamybos sektorių iki programinės įrangos ir paslaugų. Tam tikru mastu tai jau vyksta. Europoje pagaminama daugiau kaip ketvirtadalis visų pramonėje ir profesinėje aplinkoje naudojamų robotų (pvz., tiksliojo ūkininkavimo, saugumo, sveikatos, logistikos) ir ji atlieka svarbų vaidmenį kuriant ir naudojant įmonėms ir organizacijoms skirtą programinę įrangą (taikomąsias B2B programas, pvz., įmonės išteklių planavimo, projektavimo ir inžinerijos), taip pat taikomąsias e. valdžios ir išmaniosios įmonės programas.

Europa pirmąją diegiant DI gamyboje. Daugiau kaip pusė pagrindinių gamintojų gamybos operacijoms naudoja bent vieną DI produktą⁹.

Viena iš priežasčių, kodėl Europa užima tvirtą poziciją mokslinių tyrimų srityje, yra ES finansavimo programa, sėkmingai padedanti sutelkti veiksmus, išvengti dubliavimo ir pritraukiant viešųjų ir privačiųjų investicijų valstybėse narėse. Per pastaruosius trejus metus ES finansavimas DI moksliniams tyrimams ir inovacijoms išaugo iki 1,5 mlrd. EUR, t. y. padidėjo 70 proc., palyginti su ankstesniu laikotarpiu.

Tačiau investicijos į mokslinius tyrimus ir inovacijas Europoje vis dar sudaro tik dalelę viešųjų ir privačiųjų investicijų kituose pasaulio regionuose. 2016 m. Europoje į DI investuota apie 3,2 mlrd. EUR, o Šiaurės Amerikoje – maždaug 12,1 mlrd. EUR, Azijoje – 6,5 mlrd. EUR¹⁰. Taigi Europa turi gerokai padidinti savo investicijų lygį. Su valstybėmis narėmis parengtas Suderintas dirbtinio intelekto planas¹¹ yra geras atspirties taškas siekiant glaudinti bendradarbiavimą DI klausimais Europoje ir kurti sinergiją, kad į DI vertės grandinę būtų investuojama kuo daugiau.

3. ATEITIES GALIMYBIŲ IŠNAUDOJIMAS. KITA DUOMENŲ BANGA

Nors šiuo metu Europa kuriant vartotojams skirtas prietaikas ir interneto platformas atsilieka ir dėl to yra atsidūrusi nepalankioje konkurencinėje padėtyje, susijusioje su prieiga prie duomenų, laukiama didelių duomenų vertės ir kartotinio naudojimo įvairiuose sektoriuose permaitinimo. Pasaulyje sugeneruojamų duomenų kiekis sparčiai didėja – nuo 33 zetabaitų 2018 m. iki numatomų 175 zetabaitų 2025 m.¹² Kiekviena nauja duomenų banga yra proga Europai įsitvirtinti duomenų ekonomikoje ir tapti pasauline šios srities lydere. Be to, per artimiausius penkerius metus iš esmės keisis duomenų saugojimo ir tvarkymo būdas. Šiuo metu 80 proc. debesijos duomenų tvarkymo ir analizės procesų vykdoma duomenų centruose ir centriniuose kompiuterijos įrenginiuose, o 20 proc. – išmaniuosiuose prie tinklo jungiamuose objektuose, tokiuose kaip automobiliai, buitinės technikos prietaisai arba gamybiniai robotai, ir naudotojai po ranka esančiuose kompiuteriniuose įrenginiuose (tinklo paribio kompiuterija). Iki 2025 m. šios proporcijos turėtų labai keistis¹³.

Sritis, kurioje Europa pirmąją pasaulyje, yra mažos vartojamosios galios elektronika, labai svarbi DI reikalingiems naujos kartos specializuotiems procesoriams. Šioje rinkoje dabar dominuoja ne ES subjektai. Tai pakeisti galėtų iniciatyvos, tokios kaip Europos procesorių iniciatyva, kuria skatinama kurti mažos vartojamosios galios kompiuterines sistemas, skirtas tiek tinklo paribio, tiek naujos kartos našiajai kompiuterijai, ir siūloma steigti pagrindinių skaitmeninių technologijų bendrąją įmonę, kuri

⁹ Kiek atsilieka Japonija (30 proc.) ir JAV (28 proc.). Šaltinis: *CapGemini* (2019).

¹⁰ *10 imperatives for Europe in the age of AI and automation*, McKinsey (2017).

¹¹ COM(2018) 795.

¹² IDC (2019).

¹³ Gartner (2017).

turėtų pradėti veikti 2021 m. Europa taip pat pirmąja kuriant neuromorfinius sprendimus¹⁴, kurie puikiai tinka pramonės procesams (pramonė 4.0) ir transportui automatizuoti. Tai gali keleriopai padidinti energijos vartojimo efektyvumą.

Dėl pastaruoju metu padarytos kvantinės kompiuterijos pažangos apdorojimo pajėgumai didės eksponentiškai¹⁵. Europa gali būti šios technologijos pionierė, nes turi stiprią akademinę kvantinės kompiuterijos bazę, o Europos pramonė užima tvirtas pozicijas kuriant kvantinius simulatorius ir kvantinei kompiuterijai reikalingą programavimo aplinką. Šiuos naujus kvantinių technologijų sprendimus pritaikyti pramonės ir akademinėje sektoriuose padės Europos iniciatyvos, kurių tikslas – didinti kvantinių technologijų bandymų ir eksperimentų centrų prieinamumą.

Europa, remdamasi savo mokslinė kompetencija, ir toliau bus DI algoritmų kūrimo pažangos priešaky. Reikia įveikti prarają tarp šiuo metu atskirai plėtojamų disciplinų, pavyzdžiui, mašinų mokymosi ir giliojo mokymosi (kuriems būdingas ribotas interpretavimas, poreikis turėti daug duomenų modeliams mokytis ir mokytis iš koreliacijų) ir simbolinių metodų (kurių taisyklės kuriamos įsikišant žmogui). Simbolinės logikos derinimas su giliaisiais neuroniniais tinklais gali mums padėti geriau suprasti DI rezultatus.

4. KOMPETENCIJOS EKOSISTEMA

Siekiant sukurti kompetencijos ekosistemą, kuri galėtų padėti plėtoti DI ir jį diegti ES ekonomikoje ir viešajame administravime, reikia imtis aktyvesnių veiksmų įvairiais lygmenimis.

A. BENDRADARBIAVIMAS SU VALSTYBĖMIS NARĖMIS

2018 m. gruodžio mėn., vykdydama savo DI strategiją (priimtą 2018 m. balandžio mėn.)¹⁶, Komisija pateikė drauge su valstybėmis narėmis parengtą suderintą planą, kaip Europoje skatinti DI plėtotę ir naudojimą¹⁷.

Šiame plane siūloma apie 70 bendrų veiksmų, kad valstybės narės galėtų glaudžiau ir veiksmingiau bendradarbiauti tarpusavyje ir su Komisija svarbiausiais klausimais, pavyzdžiui, dėl mokslinių tyrimų, investicijų, diegimo rinkoje, įgūdžių ir talentų, duomenų ir tarptautinio bendradarbiavimo. Planuojama planą vykdyti iki 2027 m., bus reguliariai atliekama jo vykdymo stebėseną ir peržiūra.

Siekama kuo labiau padidinti investicijų į mokslinius tyrimus, inovacijas ir diegimą poveikį, įvertinti nacionalines DI strategijas ir kartu su valstybėmis narėmis remtis Suderintu dirbtinio intelekto planu ir jį išplėsti:

- *1 veiksmas. Komisija, atsižvelgdama į viešųjų konsultacijų dėl baltosios knygos rezultatus, pasiūlys valstybėms narėms persvarstyti suderintą planą ir jį priimti iki 2020 m. pabaigos.*

DI finansavimas ES lėšomis turėtų pritraukti investicijų ir jas sutelkti tose srityse, kuriose reikia imtis kur kas didesnio masto veiksmų, nei valstybės narės galėtų vienos pačios. Ateinančio dešimtmečio tikslas – ES kasmet pritraukti daugiau kaip 20 mlrd. EUR¹⁸ bendrų investicijų į DI. Privačiosioms ir viešosioms investicijoms paskatinti ES skirs išteklių pagal Skaitmeninės Europos programą, programą

¹⁴ Neuromorfiniai sprendimai – labai didelė integrinių grandynų sistema, imituojanti nervų sistemos neurobiologines struktūras.

¹⁵ Kvantiniai kompiuteriai bus pajėgūs greičiau nei per kelias sekundes apdoroti daug kartų didesnius duomenų rinkinius, nei šiandien gali našiausi kompiuteriai, todėl bus galima kurti naujas DI prietaikus įvairiuose sektoriuose.

¹⁶ [Dirbtinis intelektas Europai, COM\(2018\) 237.](#)

¹⁷ [Suderintas dirbtinio intelekto planas, COM\(2018\) 795.](#)

¹⁸ COM(2018) 237.

„Europos horizontas“ ir iš Europos struktūrinių ir investicijų fondų, kad būtų patenkinti mažiau išsivysčiusių regionų ir kaimo vietovių poreikiai.

Suderintame plane vienas iš pagrindinių DI principų taip pat galėtų būti visuomenės ir aplinkos gerovė. DI sistemos gali padėti spręsti opiausias problemas, įskaitant klimato kaitą ir aplinkos būklės blogėjimą. Taip pat svarbu, kad tai būtų daroma nekenkiant aplinkai. DI gali ir turėtų kritiškai įvertinti išteklių ir energijos naudojimą ir būti mokomas rinktis aplinkai naudingus sprendimus. Komisija apsvarstys galimybes kartu su valstybėmis narėmis skatinti ir populiarinti tokius DI sprendimus.

B. MOKSLO IR INOVACIJŲ BENDRUOMENĖS PASTANGŲ TELKIMAS

Europa nebegali sau leisti, kad kompetencijos centrai veiktų pavieniui ir todėl nė vienas iš jų nepasiektų tokio masto, kokio reikia norint konkuruoti su pasaulyje pirmaujančiais institutais. Būtina didesnė DI tyrimus atliekančių Europos mokslinių tyrimų centrų sinergija, jie turi jungtis į tinklus ir suvienyti savo jėgas, kad galėtų didinti kompetenciją, išlaikyti bei pritraukti geriausius mokslininkus ir kurti geriausias technologijas. Europai reikia kelrodžio mokslinių tyrimų, inovacijų ir ekspertų centro, kuris koordinuotų šias pastangas, būtų pasaulinis DI kompetencijos etalonas, galėtų pritraukti investicijų ir talentingiausių šios srities specialistus.

Centrų ir tinklų veiklos ašis turėtų būti tie sektoriai, kuriuose Europa turi potencialą tapti pasaulio lydere, pavyzdžiui, pramonė, sveikatos priežiūra, transportas, finansai, žemės ūkio maisto produktų vertės grandinės, energetika ir aplinka, miškininkystė, Žemės stebėjimo ir kosmoso technologijos. Visose šiose srityse vyksta lenktynės, kas bus pirmas pasaulyje, o Europa turi didžiulį potencialą, žinių ir patirties¹⁹. Ne mažiau svarbu sukurti bandymų ir eksperimentų centrus, kurie padėtų kurti ir vėliau diegti naujoviškas DI prietaikas.

- *2 veiksmas. Komisija sudarys sąlygas kurti kompetencijos ir bandymų centrams, kurie galėtų derinti Europos, nacionalines ir privačias investicijas; tam gali prireikti naujos teisinės priemonės. Pasaulinio lygio bandymų centrams Europoje remti Komisija siūlo skirti įspūdingą sumą pagal Skaitmeninės Europos programą, kurią prireikus papildys finansavimas, skirtas mokslinių tyrimų ir inovacijų veiklai pagal programą „Europos horizontas“, įtrauktą į 2021–2027 m. daugiametę finansinę programą.*

C. ĮGŪDŽIAI

Labai svarbus Europos požiūrio į DI akcentas yra įgūdžiai, kurių reikia kompetencijos spragoms užpildyti²⁰. Komisija netrukus pasiūlys Įgūdžių darbotvarkės patobulinimą, kad ES ekonomikos žaliaji ir skaitmeninė pertvarka būtų naudinga visiems europiečiams. Į iniciatyvas galėtų būti įtraukta parama sektorinėms reguliavimo institucijoms, kad pagerinusios savo DI įgūdžius jos galėtų veiksmingai ir rezultatyviai įgyvendinti atitinkamas taisykles. Atnaujintas Skaitmeninio švietimo veiksmų planas padės geriau panaudoti duomenis ir DI technologijas, pavyzdžiui, mokymosi ir prognozuojamosios analizės, švietimo ir mokymo sistemoms patobulinti ir pritaikyti skaitmeniniam amžiui. Planas taip pat padidins informuotumą apie DI visuose švietimo lygmenyse, kad piliečiai būtų pasirengę priimti informacija pagrįstus sprendimus, kuriems DI darys vis didesnę poveikį.

¹⁹ DI mokslinių tyrimų ir plėtotos galimybių taip pat suteiks būsimas Europos gynybos fondas ir nuolatinis struktūrizuotas bendradarbiavimas (PESCO). Šie projektai turėtų būti suderinti su DI skirtomis platesnėmis ES civilinėmis programomis.

²⁰ <https://ec.europa.eu/jrc/en/publication/academic-offer-and-demand-advanced-profiles-eu>

Kartu su valstybėmis narėmis persvarstant Suderintą dirbtinio intelekto planą prioritetas bus darbui naudojant DI reikalingų įgūdžių ugdymas ir darbuotojų kėlimas norint pasirengti DI atnešamoms permainingoms. Tai galėtų būti Etikos gairėse pateikto vertinimo klausimų sąrašo transformavimas į orientacinę DI kūrėjų mokymo programą, kurią kaip išteklių galėtų naudoti mokymo įstaigos. Ypač reikėtų dėti pastangas, kad šios srities išsilavinimą įgytų ir joje dirbtų daugiau moterų.

Kelrodis Europos DI mokslinių tyrimų ir inovacijų centras, turėdamas ką pasiūlyti, pritrauktų talentų iš viso pasaulio. Jis taip pat tobulintų ir skleistų kompetenciją ugdyti įgūdžius, kurių užuomazgos susiformavo ir kurie tobulėjo Europoje.

- *3 veiksmas. Įgyvendinant Skaitmeninės Europos programos tikslą, susijusį su aukšto lygio įgūdžiais, sukurti ir remti pirmaujančių universitetų ir kitų aukštojo mokslo įstaigų tinklus, siekiant pritraukti geriausius dėstytojus ir mokslininkus ir pasiūlyti geriausias pasaulyje DI magistrantūros programas.*

Darbuotojams ir darbdaviams reikės ne tik patobulinti savo įgūdžius, darbo vietoje jie tiesiogiai naudosis DI sistemų projektavimo ir prietaikų rezultatais. Socialinių partnerių įtraukimas bus lemiamas veiksnys užtikrinant į žmogų orientuotą požiūrį į DI darbe.

D. YPATINGAS DĖMESYS MVĮ

Svarbu užtikrinti, kad dirbtiniu intelektu galėtų naudotis MVĮ. Šiuo tikslu reikėtų toliau stiprinti skaitmeninių inovacijų centrus²¹ ir reikminę DI platformą²² ir skatinti MVĮ bendradarbiavimą. Tai pasiekti padėsianti priemonė – Skaitmeninės Europos programa. Visi skaitmeninių inovacijų centrai turėtų padėti MVĮ suprasti ir diegti DI, tačiau svarbu, kad kiekvienoje valstybėje narėje būtų bent vienas inovacijų centras, kuris specializuotųsi DI srityje.

MVĮ ir startuoliams reikės finansavimo, kad galėtų pritaikyti savo procesus arba diegti inovacijas naudodami DI. Pasiūlydama bandomąjį 100 mln. EUR vertės investicijų į DI ir blokų grandinės technologijas fondą, Komisija planuoja didinti galimybes gauti finansavimą DI plėtoti pagal programą „InvestEU“²³. DI aiškiai nurodytas kaip viena iš sričių, kurioms taikoma „InvestEU“ garantija.

- *4 veiksmas. Komisija bendradarbiaus su valstybėmis narėmis siekdama užtikrinti, kad kiekvienoje valstybėje narėje bent vienas skaitmeninių inovacijų centras specializuotųsi DI srityje. Skaitmeninių inovacijų centrai gali būti remiami Skaitmeninės Europos programos lėšomis.*
- *Komisija ir Europos investicijų fondas pirmąjį 2020 m. ketvirtį pradės bandomąjį 100 mln. EUR vertės projektą, pagal kurį bus finansuojamas novatoriško DI kūrėjų nuosavas kapitalas. Jei bus pritarta tvirtinant galutinę daugiametę finansinę programą, Komisija ketina nuo 2021 m. šį finansavimą gerokai padidinti iš programos „InvestEU“ lėšų.*

E. PARTNERYSTĖ SU PRIVAČIUOJU SEKTORIUMI

Labai svarbu užtikrinti, kad į mokslinių tyrimų ir inovacijų darbotvarkės sudarymą visapusiškai įsitrauktų ir reikiamą bendro investavimo lygį užtikrintų privatusis sektorius. Tam turi būti sudaryta

²¹ ec.europa.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities.

²² www.Ai4eu.eu.

²³ Europe.eu/investeu.

plati viešojo ir privačiojo sektorių partnerystė ir užtikrintas įmonių aukščiausiosios vadovybės įsipareigojimas.

- *5 veiksmas. Vykdydama programą „Europos horizontas“, Komisija sukurs naują – DI, duomenų ir robotikos – viešojo ir privačiojo sektorių partnerystės organizaciją, kuri sutelks pastangas, koordinuos DI mokslinius tyrimus ir inovacijas, bendradarbiaus su kitomis pagal programą „Europos horizontas“ sukurtomis viešojo ir privačiojo sektorių partnerystės organizacijomis ir su minėtais bandymų centrais bei skaitmeninių inovacijų centrais.*

F. SKATINIMAS DI DIEGTI VIEŠAJAME SEKTORIJE

Labai svarbu, kad viešojo administravimo institucijos, ligoninės, komunalinių ir transporto paslaugų įmonės, finansų priežiūros institucijos ir kiti viešieji subjektai savo veikloje pradėtų sparčiai diegti DI produktus ir paslaugas. Ypač svarbios sritys bus sveikatos priežiūra ir transportas – jose jau turima brandžių technologijų, kurias galima plačiai diegti.

- *6 veiksmas. Komisija inicijuos atvirus ir skaidrius sektorinius dialogus, pirmenybę teikdama sveikatos priežiūrai, kaimo vietovių administravimo įstaigoms ir viešųjų paslaugų teikėjams, kad pateiktų veiksmų planą, kuriuo būtų sudarytos palankesnės kūrimo, eksperimentavimo ir diegimo sąlygos. Vykdamas sektorinius dialogus bus rengiama speciali DI diegimo programa, kuri padės vykdyti DI sistemų viešuosius pirkimus ir pertvarkyti pačius viešųjų pirkimų procesus.*

G. PRIEIGOS PRIE DUOMENŲ IR KOMPIUTERIJOS INFRASTRUKTŪROS UŽTIKRINIMAS

Šioje baltojoje knygoje aptariamos veiksmų sritys papildo kartu su ja skelbiamos Europos duomenų strategijos planą. Labai svarbu gerinti prieigą prie duomenų ir jų tvarkymą. Be duomenų neįmanoma kurti DI ir kitų skaitmeninių prietaikų. Milžiniškas naujų duomenų, kurie turės būti sugeneruoti, kiekis yra proga Europai įsitvirtinti priešakinėse duomenų ir DI transformacijos linijose. Propaguojant atsakingą duomenų tvarkymą ir sąžiningo duomenų naudojimo (FAIR) principų laikymąsi didės pasitikėjimas ir bus užtikrinamas kartotinis duomenų naudojimas²⁴. Ne mažiau svarbu investuoti į bazines kompiuterijos technologijas ir infrastruktūrą.

Komisija Skaitmeninės Europos programoje pasiūlė daugiau kaip 4 mlrd. EUR skirti našiai ir kvantinei kompiuterijai, įskaitant tinklo paribio kompiuteriją ir DI, duomenų ir debesijos infrastruktūrą. Šie prioritetai labiau detalizuojami Europos duomenų strategijoje.

H. TARPTAUTINIAI ASPEKTAI

Europa turi geras galimybes būti pasauline lydere sudarydama bendromis vertybėmis grindžiamas sąjungas ir propaguodama etišką DI naudojimą. DI srityje nuveiktas ES darbas jau davė peno tarptautinėms diskusijoms. Etikos gaires rengusi Aukšto lygio ekspertų grupė pasitelkė nemažai ne ES organizacijų ir keletą vyriausybinių stebėtojų. Savo ruožtu ES aktyviai dalyvavo formuluojant EBPO

²⁴ Surandami, prieinami, sąveikūs ir kartotiniai naudojami (*Findable, Accessible, Interoperable and Reusable*, FAIR), Komisijos sąžiningo duomenų naudojimo ekspertų grupės galutinė ataskaita ir veiksmų planas, 2018 m., https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

dirbtinio intelekto etikos principus²⁵. Didysis dvidešimtukas šiuos principus patvirtino 2019 m. birželio mėn. Ministrų pareiškimė dėl prekybos ir skaitmeninės ekonomikos.

ES taip pat pripažįsta, kad svarbų darbą DI srityje vykdo kiti daugiašaliai forumai, tarp jų – Europos Taryba, Jungtinių Tautų švietimo, mokslo ir kultūros organizacija (UNESCO), Ekonominio bendradarbiavimo ir plėtros organizacija (EBPO), Pasaulio prekybos organizacija ir Tarptautinė telekomunikacijų sąjunga (ITU). ES dalyvauja Jungtinėms Tautoms svarstant tolesnes priemones, susijusias su Aukšto lygio komisijos skaitmeninio bendradarbiavimo klausimais parengta ataskaita, įskaitant jos rekomendaciją dėl DI.

ES dėl DI toliau bendradarbiaus su bendramintėmis šalimis ir su pasauliniais subjektais laikydamasi ES taisyklėmis ir vertybėmis grindžiamo požiūrio (pvz., palaikydama aukštynkryptę reguliavimo konvergenciją, prieigą prie pagrindinių išteklių, įskaitant duomenis, vienuodų sąlygų sudarymą). Komisija atidžiai stebės trečiųjų valstybių politiką, kuria ribojami duomenų srautai, ir nepagrįstus apribojimus sieks šalinti vykdydama dvišales prekybos derybas ir imdamasi veiksmų Pasaulio prekybos organizacijoje. Komisija yra įsitikinusi, kad tarptautinis bendradarbiavimas DI klausimais turi būti grindžiamas požiūriu, skatinančiu gerbti pagrindines teises, įskaitant teisę į orumą, pliuralizmą, įtrauktį, nediskriminavimą, privatumo ir asmens duomenų apsaugą²⁶, ir stengsis savo vertybes propaguoti visame pasaulyje²⁷. Taip pat aišku, kad atsakingas DI plėtojimas ir naudojimas gali būti varomoji jėga siekiant darnaus vystymosi tikslų ir įgyvendinant Darbotvarkę iki 2030 m.

5. PASITIKĖJIMO EKOSISTEMA. DI REGLAMENTAVIMO SISTEMA

Kaip ir bet kuri nauja technologija, DI ne tik atveria galimybių, bet ir atneša pavojų. Piliečiai baiminasi, kad dėl algoritminio sprendimų priėmimo informacijos asimetrijos turės mažiau galių apginti savo teises ir užsitikrinti saugą, o įmonės yra susirūpinusios dėl teisinio netikrumo. Nors DI gali padėti apsaugoti piliečius ir suteikti jiems galimybę naudotis savo pagrindinėmis teisėmis, piliečiai taip pat nerimauja, kad DI gali turėti nepageidaujamą poveikį ar net būti naudojamas piktavališkais tikslais. Į šį nerimą reikia reaguoti. Be to, trūksta ne tik investicijų ir įgūdžių, pagrindinis veiksnys, stabdantis platesnį DI naudojimą, yra pasitikėjimo stoka.

Todėl 2018 m. balandžio 25 d. Komisija priėmė dirbtinio intelekto strategiją²⁸, kurioje išnagrinėti socialiniai ir ekonominiai aspektai, taip pat poreikis didinti investicijas į mokslinius tyrimus, inovacijas ir DI pajėgumus visoje ES. Ji sutarė su valstybėmis narėmis dėl Suderinto plano²⁹ strategijoms suderinti. Komisija taip pat sudarė Aukšto lygio ekspertų grupę, kuri 2019 m. balandžio mėn. paskelbė Patikimo dirbtinio intelekto etikos gaires³⁰.

Komisija paskelbė komunikatą³¹, kuriame palankiai įvertino septynis pagrindinius reikalavimus, nustatytus Aukšto lygio ekspertų grupės gairėse:

- žmogiškasis veiksnys ir žmogaus atliekama priežiūra,
- techninis patvarumas ir saugumas,
- privatumas ir duomenų valdymas,

²⁵ <https://www.oecd.org/going-digital/ai/principles/>

²⁶ Taikydama partnerystės priemonę, Komisija skirs 2,5 mln. EUR bendradarbiavimo su bendraminčiais partneriais projektui, kurio tikslas – populiarinti ES DI etikos gaires, patvirtinti bendrus principus ir padaryti praktines išvadas.

²⁷ Pirmininkė U. von der Leyen, „Daugiau siekianti Sąjunga. Mano Europos darbotvarkė“, 17 p.

²⁸ COM(2018) 237.

²⁹ COM(2018) 795.

³⁰ <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>

³¹ COM(2019) 168.

- skaidrumas,
- įvairovė, nediskriminavimas ir teisingumas,
- visuomenės ir aplinkos gerovė,
- atskaitomybė.

Gairėse taip pat pateikiamas praktinėms įmonių reikmėms skirtas vertinimo klausimų sąrašas. Per antrąjį 2019 m. pusmetį šį vertinimo klausimų sąrašą išbandė ir atsiliepimus atsiuntė daugiau kaip 350 organizacijų. Aukšto lygio grupė gaires šiuo metu peržiūri atsižvelgdama į gautus atsiliepimus ir baigs šį darbą iki 2020 m. birželio mėn. Iš atsiliepimų visų pirma aiškėja, kad nors galiojančiais teisės aktais ar reguliavimo tvarka daug reikalavimų jau yra nustatyti, dabartiniuose daugelio ekonomikos sektorių teisės aktuose nėra konkrečių skaidrumo, atsekamumo ir žmogaus atliekamos priežiūros reikalavimų.

Kartu su šiomis neprivalomomis Aukšto lygio ekspertų grupės gairėmis ir Pirmininkės politinėmis gairėmis aiški Europos reglamentavimo sistema sustiprintų vartotojų ir įmonių pasitikėjimą dirbtiniu intelektu ir jo technologijos būtų diegiamos sparčiau. Tokia reglamentavimo sistema turėtų derėti su kitais veiksmais Europos inovaciniam pajėgumui ir konkurencingumui šioje srityje didinti. Be to, ji turi užtikrinti socialiniu, aplinkos ir ekonominiu požiūriu optimalius rezultatus ir atitikti ES teisės aktams, principams ir vertybėms. Tai ypač svarbu tose srityse, kuriose piliečių teisėms gali būti daromas didžiausias tiesioginis poveikis, pavyzdžiui, naudojant DI prietaikas teisėsaugos ir teisminių institucijų reikmėms.

DI kūrėjams ir diegėjams jau taikomi Europos teisės aktai dėl pagrindinių teisių (pvz., duomenų apsaugos, privatumo, nediskriminavimo), vartotojų apsaugos, gaminių saugos ir atsakomybės taisyklės. Vartotojai tikisi tokio pat saugos lygio ir pagarbos jų teisėms, nepriklausomai nuo to, ar produktas arba sistema grindžiamas DI, ar ne. Tačiau dėl tam tikrų DI ypatumų (pvz., neskaidrumo) šiuos teisės aktus gali būti sunkiau taikyti ir užtikrinti jų vykdymą. Dėl šios priežasties reikia išnagrinėti, ar galiojančiais teisės aktais galima mažinti DI keliamą riziką ir ar galima veiksmingai užtikrinti jų vykdymą, ar teisės aktus reikia pritaikyti, o gal reikia naujų teisės aktų.

Atsižvelgiant į sparčią DI plėtotę, reglamentavimo sistemoje turi būti numatyta vėlesnių patobulinimų galimybė. Pakeitimai turėtų apsiriboti aiškiai nustatytais problemomis, kurias galima racionaliai išspręsti.

Valstybės narės atkreipia dėmesį į tai, kad šiuo metu bendros europinės sistemos nėra. Vokietijos duomenų etikos komisija paragino sukurti riziką grindžiamą reglamentavimo sistemą, sudarytą iš penkių lygmenų: visai nereglementuoti nekenksmingiausių DI sistemų, o pavojingiausias visiškai uždrausti. Danija ką tik sukūrė duomenų etikos ženklo prototipą. Malta įvedė savanoriško DI sertifikavimo sistemą. Jei ES nesuformuluos europinio požiūrio, yra realus vidaus rinkos susiskaidymo pavojus ir tai trukdytų siekti pasitikėjimo, teisinio tikrumo ir diegimo rinkoje tikslų.

Tvirta europinė patikimo DI reglamentavimo sistema apsaugos visus Europos piliečius ir padės kurti sklandžiai veikiančią vidaus rinką, kad būtų galima toliau plėtoti ir diegti DI ir stiprinti Europos pramoninę DI bazę.

A. PROBLEMŲ APIBŪDINIMAS

Nors DI gali būti labai naudingas, be kita ko, padaryti produktus ir procesus saugesnius, jis gali padaryti ir žalos. Ši žala gali būti materialinė (žala asmenų saugai ir sveikatai, įskaitant gyvybės praradimą, turtinę žalą) ir nematerialinė (privatumo netekimas, teisės į saviraiškos laisvę apribojimai, žmogaus orumo pažeidimas, diskriminacija, pavyzdžiui, įsidarbinant) ir gali būti susijusi su įvairiausiais pavojais. Reglamentavimo sistemoje daugiausia dėmesio turėtų būti skiriama tam, kaip kuo labiau sumažinti įvairių galimos žalos riziką, visų pirma pačią didžiausią.

Pagrindinė DI keliama rizika yra susijusi su taisyklių, skirtų pagrindinėms teisėms (įskaitant asmens duomenų ir privatumo apsaugą bei nediskriminavimą) apsaugoti, taikymu, taip pat su sauga³² ir atsakomybe.

Pagrindinėms teisėms, įskaitant teisę į asmens duomenų bei privatumo apsaugą ir nediskriminavimą, kylanti rizika

DI naudojimas gali daryti poveikį pamatinėms ES vertybėms ir pažeisti pagrindines teises³³, įskaitant teisę į saviraiškos laisvę, susirinkimų laisvę, žmogaus orumą, nediskriminavimą dėl lyties, rasinės arba etninės kilmės, religijos ar tikėjimo, negalios, amžiaus arba seksualinės orientacijos, kai tai aktualu tam tikrose srityse, teisę į asmens duomenų ir privatumo apsaugą³⁴ arba teisę į veiksmingą teisminę gynybą ir teisingą bylos nagrinėjimą, taip pat neatitikti vartotojų apsaugos taisyklių. Ši rizika gali kilti dėl to, kad yra bendrųjų DI sistemų projektavimo trūkumų (be kita ko, susijusių su žmogaus atliekama priežiūra), arba dėl to, kad naudojami neobjektyvūs duomenys (pvz., sistemai mokytis naudojami tik arba daugiausia vyrų duomenys, todėl moterų atžvilgiu gaunami neoptimalūs rezultatai).

DI gali atlikti daug funkcijų, kurias anksčiau galėjo atlikti tik žmogus. Todėl fiziniai ir juridiniai asmenys vis dažniau susidurs su veiksmais ir sprendimais, kurie bus priimami DI sistemų arba jomis naudojantis ir kuriuos kartais gali būti sunku suprasti ir prireikus veiksmingai užginčyti. Be to, DI suteikia daugiau galimybių stebėti ir analizuoti kasdienes žmonių įpročius. Pavyzdžiui, esama rizikos, kad valstybės institucijos ar kiti subjektai, pažeisdami ES duomenų apsaugos ir kitas taisykles, gali naudoti DI masinio sekimo tikslais, o darbdaviai – stebėti, kaip elgiasi jų darbuotojai. Analizuojant didelius duomenų kiekius ir nustatant jų sąsajas, DI taip pat gali būti naudojamas asmens duomenims atsekti ir išanoniminti, taip iškiltų naujo pobūdžio pavojus asmens duomenų apsaugai net ir tada, kai pačiuose duomenų rinkiniuose asmens duomenų nėra. Interneto tarpininkai taip pat naudoja DI siekdami nustatyti naudotojus dominančios informacijos prioritetus ir parinkti jiems turinį. Tai, kaip tvarkomi duomenys, projektuojamos prietaikos ir kokią galimybę įsikišti turi žmogus, gali turėti įtakos teisėms į saviraiškos laisvę, asmens duomenų apsaugą bei privatumą ir politinėms laisvėms.

³² Tai gali būti kibernetinio saugumo, DI prietaikų naudojimo ypatingos svarbos infrastruktūros objektuose arba piktavališko DI naudojimo problemos.

³³ Europos Tarybos tyrimai rodo, kad DI gali daryti poveikį daugeliui pagrindinių teisių. <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>.

³⁴ Šiai rizikai mažinti priimtas Bendrasis duomenų apsaugos reglamentas (BDAR) ir E. privatumo direktyva (deramasi dėl naujo e. privatumo reglamento), tačiau gali reikėti išnagrinėti, ar DI sistemos nekelia daugiau rizikos. Komisija nuolat stebės BDAR taikymą ir jį vertins.

Kai kuriems DI algoritmams, naudojamiems nusikaltimų recidyvui prognozuoti, gali būti būdingas neobjektyvumas lyties ar rasės pagrindu, dėl kurio skirtingai nustatoma moterų ir vyrų arba piliečių ir užsieniečių recidyvo tikimybė. Šaltinis: Tolan S., Miron M., Gomez E. and Castillo C. „Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia“, Best Paper Award, International Conference on AI and Law, 2019

Kai kurioms veido analizei skirtoms DI programoms būdingas neobjektyvumas lyties ar rasės pagrindu, dėl kurio analizuojant šviesesnės odos vyrų veidus daroma nedaug lyties nustatymo klaidų, tačiau daug jų daroma analizuojant tamsesnės odos moterų veidus. Šaltinis: Joy Buolamwini, Timnit Gebru; *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81:77-91, 2018.

Tendencingumas ir diskriminacija yra bet kuriai visuomeninei ar ekonominei veiklai būdinga rizika. Žmogus, priimdamas sprendimus, nėra apsaugotas nuo klaidų ir neobjektyvumo. Tačiau DI neobjektyvumo padariniai galėtų būti kur kas didesni, dėl jo gali nukentėti ir būti diskriminuojami daug žmonių, nes nėra socialinės kontrolės mechanizmų, reguliuojančių žmonių elgesį³⁵. Taip gali atsitikti ir tada, kai DI sistema vienu metu ir veikia, ir „mokosi“. Tais atvejais, kai nepageidaujamų rezultatų negalima išvengti ar numatyti projektavimo etape, rizika kyla ne dėl pirminio sistemos projekto trūkumų, o dėl praktinio koreliacijų ar dėsningumų, kuriuos sistema nustato iš didelio duomenų rinkinio, poveikio.

Dėl daugeliui DI technologijų būdingų ypatybių, tokių kaip neskaidrumas (juodosios dėžės reiškinys), sudėtingumas, nenusipėjamumas ir dalinis autonomiškumas, gali būti sunku patikrinti jų atitiktį galiojančių ES teisės aktų, kuriais siekiama apsaugoti pagrindines teises, taisyklėms ir tai gali trukdyti veiksmingai užtikrinti jų vykdymą. Vykdomo užtikrinimo institucijoms ir poveikį patyrusiems asmenims gali trūkti priemonių patikrinti tai, kaip tam tikras sprendimas buvo priimtas naudojant DI, taigi ir tai, ar laikytasi atitinkamų taisyklių. Dėl tokių sprendimų nukentėjusiems fiziniams ir juridiniams asmenims gali kilti sunkumų veiksmingai pasinaudoti teise kreiptis į teismą.

Pavojus saugai ir veiksmingam atsakomybės užtikrinimui

DI technologijos, integruojamos į produktus ir paslaugas, gali kelti naujo pobūdžio pavojų naudotojų saugai. Pavyzdžiui, dėl objekto atpažinimo technologijos trūkumų savivaldis automobilis gali neteisingai atpažinti objektą kelyje ir sukelti eismo įvykį, per kurį sužeidžiami žmonės ir padaroma materialinė žala. Šis pavojus, kaip ir pavojus pagrindinėms teisėms, gali kilti dėl DI technologijos projektavimo trūkumų, dėl duomenų prieinamumo ir kokybės problemų arba kitų su mašinų mokymusi susijusių problemų. Nors kai kurie iš šių pavojų būdingi ne tik DI produktams ir paslaugoms, dėl DI naudojimo pavojus gali dar padidėti.

Nesant aiškių saugos nuostatų pavojams pašalinti, gali kilti pavojus ne tik tam tikriems asmenims, bet ir atsirasti teisinis netikrumas įmonėms, Europos Sąjungoje parduodančioms savo produktus, kuriems

³⁵ Komisijos Moterų ir vyrų lygių galimybių patariamasis komitetas šiuo metu rengia nuomonę dėl dirbtinio intelekto, kurioje, be kito poveikio, analizuojamas DI poveikis lyčių lygybei, ir planuoja ją priimti 2020 m pradžioje. DI ir lyčių lygybės ryšys taip pat nagrinėjamas 2020–2024 m. ES lyčių lygybės strategijoje 2020 m pradžioje Europos nacionalinių lygybės įstaigų tinklas (EQUINET) planuoja paskelbti (Robino Alleno ir Dee Masters) ataskaitą „Regulating AI: the new role for Equality Bodies – Meeting the new challenges to equality and non-discrimination from increased digitalisation and the use of AI“.

naudojamas DI. Rinkos priežiūros ir vykdymo užtikrinimo institucijoms gali būti neaišku, ar jos gali įsikišti, nes jos gali neturėti įgaliojimų veikti ir (arba) tinkamų techninių galimybių patikrinti sistemas³⁶. Taigi dėl teisinio netikrumo gali sumažėti bendras saugos lygis ir Europos įmonių konkurencingumas.

Jei kiltų realus pavojus saugai, nesant aiškių reikalavimų ir dėl minėtų DI technologijų savybių būtų sunku atsekti potencialius problemiškus sprendimus, priimtus naudojant DI sistemas. Dėl to žalą patyrusiems asmenims gali būti sunku gauti kompensaciją pagal dabartinius ES ir nacionalinės teisės aktus dėl atsakomybės³⁷.

Pagal Atsakomybės už gaminius direktyvą už žalą dėl gaminio trūkumų atsako gamintojas. Tačiau DI sistemų, kaip antai savivaldžių automobilių, atveju gali būti sunku įrodyti, jog gaminys turi trūkumų, buvo padaryta žala ir tarp šių dviejų dalykų yra priežastinis ryšys. Be to, neaišku, kaip ir koku mastu Atsakomybės už gaminius direktyva taikoma tam tikrų rūšių trūkumams, pavyzdžiui, jei jų atsiranda dėl gaminio kibernetinio saugumo spragų.

Taigi, kalbant apie pagrindines teises paminėtas sunkumas atsekti DI sistemų priimtus potencialius problemiškus sprendimus yra lygiai toks pats aktualus sprendžiant saugos ir atsakomybės klausimus. Žalą patyrę asmenys gali neturėti veiksmingos prieigos prie įrodymų, kurie yra būtini, pavyzdžiui, norint kreiptis į teismą, ir gali turėti mažiau galimybių veiksmingai apginti savo teises nei tais atvejais, kai žala padaroma naudojant tradicines technologijas. Tokių rizika didės, nes DI naudojamas vis plačiau.

B. GALIMI GALIOJANČIŲ ES TEISĖS AKTŲ PATIKSLINIMAI, SUSIJĘ SU DI

ES turi daug teisės aktų, kuriais reglamentuojama gaminių sauga ir atsakomybė už juos³⁸, įskaitant konkretiems sektoriams taikomas taisykles, kuriuos papildo nacionalinės teisės aktai ir kurie yra aktualūs ir potencialiai taikytini kai kurioms naujoms DI prietaikoms.

Pagrindinėms teisėms ir vartotojų teisėms apsaugoti skirti ES teisės aktai yra Rasinės lygybės direktyva³⁹, Direktyva dėl vienodo požiūrio užimtumo ir profesinėje srityje⁴⁰, direktyvos, kuriomis įgyvendinamas vienodo požiūrio į moteris ir vyrus principas užimtumo srityje ir dėl galimybės naudotis prekėmis bei paslaugomis⁴¹, įvairios vartotojų apsaugos taisyklės⁴², asmens duomenų ir privatumo apsaugos taisyklės, visų pirma Bendrasis duomenų apsaugos reglamentas ir kiti sektoriai

³⁶ Vienas iš pavyzdžių galėtų būti vaikiškas išmanusis laikrodis. Šis gaminys jį seginčiam vaikui gali nedaryti tiesioginės žalos, tačiau, neužtikrinus būtinojo saugumo lygio, jį galima lengvai naudoti kaip prieigos prie vaiko priemonę. Rinkos priežiūros institucijoms gali būti sunku įsikišti tais atvejais, kai pavojus nėra susijęs su pačiu gaminiu.

³⁷ Poreikis DI, daiktų internetą ir kitas skaitmenines technologijas įtraukti į teisės aktus, kuriais reglamentuojama sauga ir atsakomybė, analizuojamas kartu su šia baltąja knyga skelbiamoje Komisijos ataskaitoje.

³⁸ ES teisės aktai, kuriais reglamentuojama gaminių sauga, yra Direktyva dėl bendros gaminių saugos (Direktyva 2001/95/EB), kuria sukurta apsaugos sistema, ir daug sektorinių taisyklių, taikomų įvairių kategorijų gaminiams, nuo mašinų, lėktuvų ir automobilių iki žaislų ir medicinos priemonių, skirtų aukštam sveikatos apsaugos ir saugos lygiui užtikrinti. Atsakomybę už gaminius reglamentuojančius teisės aktus papildo įvairios civilinės atsakomybės už gaminių ar paslaugų padarytą žalą sistemos.

³⁹ Direktyva 2000/43/EB.

⁴⁰ Direktyva 2000/78/EB.

⁴¹ Direktyva 2004/113/EB; Direktyva 2006/54/EB.

⁴² Pavyzdžiui, Nesąžiningos komercinės veiklos direktyva (Direktyva 2005/29/EB) ir Vartotojų teisių direktyva (Direktyva 2011/83/EB).

asmens duomenų apsaugos teisės aktai, kaip antai Duomenų apsaugos teisės saugos srityje direktyva⁴³. Be to, nuo 2025 m. bus taikomos Europos prieinamumo akte⁴⁴ nustatytos prekių ir paslaugų prieinamumo reikalavimų taisyklės. Į pagrindines teises atsižvelgiama ir įgyvendinant kitus ES teisės aktus, be kita ko, finansinių paslaugų, migracijos ar interneto tarpininkų atsakomybės srityse.

Nors ES teisės aktai iš esmės ir toliau visapusiškai taikomi, nepriklausomai nuo to, ar gaminiams naudojamas DI, svarbu įvertinti, ar jų vykdymo užtikrinimo pakanka DI sistemų keliamiems pavojams pašalinti, ar reikia pritaikyti konkrečias teisines priemones.

Pavyzdžiui, visa atsakomybė už DI atitiktį galiojančioms vartotojų apsaugos taisyklėms ir toliau tenka ekonominės veiklos vykdytojams, draudžiama algoritminę vartotojų elgsenos analizę naudoti pažeidžiant galiojančias taisykles ir už pažeidimus atitinkamai baudžiama.

Komisija laikosi nuomonės, kad teisės aktai galėtų būti patobulinti siekiant spręsti toliau nurodytas problemas ir mažinti su jomis siejamą riziką:

- *Veiksmingas galiojančių ES ir nacionalinės teisės aktų taikymas ir vykdymo užtikrinimas.* Dėl pagrindinių DI ypatumų kyla sunkumų užtikrinti tinkamą ES ir nacionalinės teisės aktų taikymą ir vykdymą. Dėl nepakankamo DI skaidrumo sunku nustatyti ir įrodyti, kad buvo pažeisti teisės aktai, be kita ko, teisės nuostatos, kuriomis saugomos pagrindinės teisės, nustatoma atsakomybė ir sąlygos, kuriomis galima reikalauti kompensacijos. Todėl galiojančius tam tikrų sričių teisės aktus, pavyzdžiui, dėl atsakomybės, gali prireikti patikslinti arba paaiškinti, kad būtų užtikrintas veiksmingas jų taikymas ir vykdymas; tai išsamiau aptariama kartu su šia baltąja knyga skelbiamoje ataskaitoje.
- *Galiojančių ES teisės aktų taikymo srities apribojimai.* ES gaminių saugos teisės aktuose pagrindinis dėmesys skiriamas gaminių pateikimui rinkai. Nors pagal ES gaminių saugos teisės aktus programinė įranga, kai ji yra galutinio gaminio dalis, turi atitikti atitinkamų gaminių saugos taisykles, neaišku, išskyrus kai kuriuos sektorius, kuriuose nustatytos aiškos taisyklės⁴⁵, ar ES gaminių saugos teisės aktai taikomi autonominei programinei įrangai. Šiuo metu galiojantys bendrieji ES saugos teisės aktai taikomi gaminiams, o ne paslaugoms, todėl iš principo jie netaikomi ir DI technologijomis grindžiamoms paslaugoms (pvz., sveikatos priežiūros, finansinėms, transporto paslaugoms).
- *DI intelekto sistemų funkcijų keitimas.* Produktų ir sistemų, į kuriuos integruota programinė įranga, įskaitant DI, veikimas per visą jų gyvavimo ciklą gali kisti. Tai ypač pasakytina apie sistemas, kurių programinę įrangą reikia dažnai atnaujinti arba kurios grindžiamos mašinų mokymusi. Dėl šių savybių gali kilti naujo pobūdžio pavojų, kurių nebuvo, kai sistema buvo pateikiama rinkai. Į šiuos pavojus nėra tinkamai atsižvelgta galiojančiuose teisės aktuose, juose daugiausia dėmesio skiriama tiems saugos pavojams, kurie yra žinomi pateikimo rinkai metu.

⁴³ 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.

⁴⁴ Direktyva (ES) 2019/882 dėl gaminių ir paslaugų prieinamumo reikalavimų.

⁴⁵ Pavyzdžiui, programinė įranga, gamintojo numatyta naudoti medicinos tikslais, laikoma medicinos priemone pagal Medicinos priemonių reglamentą (Reglamentą (ES) 2017/745).

- *Netikrumas dėl atsakomybės paskirstymo įvairiems tiekimo grandinės ekonominės veiklos vykdytojams.* Pagal ES gaminių saugos teisės aktus atsakomybė paprastai tenka rinkai pateikiamo gaminio, įskaitant visas jo sudedamąsias dalis, pavyzdžiui, DI sistemas, gamintojui. Tačiau taisyklės gali pasidaryti neaiškios, jei DI į rinkai pateiktą gaminį integruoja subjektas, kuris nėra gamintojas. Be to, ES teisės aktuose dėl atsakomybės už gaminius numatyta gamintojų atsakomybė, o kitų tiekimo grandinės dalyvių atsakomybė reglamentuojama nacionalinėmis atsakomybės taisyklėmis.
- *Saugos sąvokos pokyčiai.* DI naudojimas produktams ir paslaugoms gali kelti pavojų, kurie šiuo metu nėra aiškiai aptariami ES teisės aktuose. Tai gali būti kibernetinės grėsmės, pavojus asmens saugumui (kurį gali kelti naujos DI prietaikos, pavyzdžiui, buitinėje technikoje), rizika nutrūkus ryšiui ir t. t. Šie pavojai gali būti žinomi gaminių pateikimo rinkai metu arba jų gali atsirasti jau naudojant gaminį – dėl programinės įrangos atnaujinimo ar savimokos. Kad sustiprintų su DI prietaikomis siejamos potencialios rizikos įrodymų bazę, ES turėtų visapusiškai panaudoti turimas priemones, be kita ko, remtis ES kibernetinio saugumo agentūros (ENISA) patirtimi, sukaupia vertinant DI grėsmes.

Kaip minėta, kelios valstybės narės jau nagrinėja galimybes priimti nacionalinės teisės aktus DI keliamoms problemoms spręsti. Todėl kyla pavojus, kad bendroji rinka gali susiskaidyti. Skirtingos nacionalinės taisyklės gali būti kliūtis įmonėms, norinčioms parduoti ir naudoti DI sistemas bendrojoje rinkoje. Užtikrinus bendrą požiūrį ES lygmeniu, Europos įmonės galėtų sklandžiai įsiliesti į bendrąją rinką ir būtų konkurencingesnės pasaulio rinkose.

Ataskaita dėl DI, daiktų interneto ir robotikos poveikio saugai ir atsakomybei

Kartu su šia baltąja knyga skelbiamoje ataskaitoje analizuojami susiję teisės aktai. Joje nurodyti jų taikymo neaiškumai, susiję su konkrečiais DI sistemų ir kitų skaitmeninių technologijų keliamais pavojais.

Ataskaitoje daroma išvada, kad galiojančiuose gaminių saugos teisės aktuose jau palaikoma platesnė saugos koncepcija siekiant apsidrausti nuo visų rūšių rizikos dėl gaminio naudojimo pagal jo paskirtį. Tačiau, siekiant užtikrinti didesnę teisinę tikrumą, galėtų būti įtrauktos nuostatos, kuriomis būtų aiškiai reglamentuojami besiformuojančių skaitmeninių technologijų keliama naujo pobūdžio pavojai.

- Tam tikrų DI sistemų autonomiškumas gali lemti svarbius gaminio pokyčius per jo gyvavimo ciklą, darančius poveikį saugai, todėl gali reikėti atlikti naują rizikos vertinimą. Be to, gali būti, kad kaip apsaugos priemonė yra būtina žmogaus atliekama priežiūra tiek gaminio projektavimo etapu, tiek per visą DI produktų ir sistemų gyvavimo ciklą.
- Taip pat būtų galima apsvarstyti galimybę nustatyti aiškius įpareigojimus gamintojams, susijusius su naudotojų psichiniu saugumu, kai tai aktualu (pvz., bendravimas su robotais humanoidais).
- Sąjungos gaminių saugos teisės aktuose galėtų būti nustatyti konkretūs reikalavimai, kuriais projektavimo etapu būtų mažinamas pavojus saugai dėl klaidingų duomenų, taip pat mechanizmai, kuriais būtų užtikrinama, kad duomenų kokybė būtų išlaikyta visą DI produktų ir sistemų naudojimo laiką.
- Algoritminių sistemų neskaidrumo problema galėtų būti sprendžiama taikant skaidrumo reikalavimus.
- Galiojančias taisykles gali reikėti pritaikyti ir patikslinti tuo atveju, kai autonominė programinė įranga pateikiama rinkai arba jau pateikta rinkai atsisiunčiamą į gaminį, jei tai daro poveikį saugai.
- Atsižvelgiant į tai, kad naujų technologijų tiekimo grandinės vis sudėtingėja, teisinę tikrumą galėtų užtikrinti nuostatos, kuriomis reikalaujama, kad tiekimo grandinėje dalyvaujantys ekonominės veiklos vykdytojai ir naudotojai bendradarbiautų.

Besiformuojančios skaitmeninės technologijos, tokios kaip DI, daiktų internetas ir robotika, dėl savo ypatybių gali kelti sunkumų taikyti atsakomybės sistemas ir mažinti jų veiksmingumą. Dėl kai kurių jų ypatybių gali būti sunku nustatyti žalą sukėlusį asmenį, o tai pagal daugumą nacionalinių taisyklių būtina norint pareikalauti kompensacijos dėl trūkumų. Dėl to gali labai padidėti nukentėjusių asmenų išlaidos ir gali būti sunku įrodyti žalą ir ją išieškoti ne iš gamintojo, o iš kitų asmenų.

- Asmenims, patyrusiems žalą dėl DI sistemų, turi būti taikoma tokio paties lygio apsauga kaip ir asmenims, patyrusiems žalą dėl kitų technologijų, tačiau neturėtų būti trukdoma technologinių inovacijų plėtotė.
- Turėtų būti atidžiai įvertintos visos galimybės užtikrinti tokią apsaugą, taip pat ir galimybė iš dalies pakeisti Atsakomybės už gaminius direktyvą ir tikslingiau suderinti nacionalines atsakomybės taisykles. Pavyzdžiui, Komisija siekia išsiaiškinti, ar ir koku mastu reikėtų sušvelninti tokių sudėtingų situacijų pasekmes, t. y. pritaikyti nuostatas, dėl nacionalinėse atsakomybės taisyklėse nustatytos pareigos įrodyti žalą, kai ji padaroma naudojantis DI prietaikomis.

Atsižvelgdama į pirmiau pateiktus argumentus, Komisija daro išvadą, kad gali prireikti ne tik tikslinti galiojančius teisės aktus, bet ir naujų, konkrečiai DI taikytinų, teisės aktų, kad ES teisės aktų sistema tinkamai aprėptų dabartinius ir numatomus technologinius ir komercinius pokyčius.

C. BŪSIMOS ES REGLAMENTAVIMO SISTEMOS APRĖPTIS

Vienas iš pagrindinių būsimos specialios DI reglamentavimo sistemos klausimų – nustatyti jos taikymo aprėptį. Daroma pradinė prielaida, kad reglamentavimo sistema būtų taikoma DI produktams ir paslaugoms. Todėl šioje baltojoje knygoje ir visose būsimose politikos iniciatyvose dirbtinis intelektas turėtų būti aiškiai apibrėžtas.

Pirmąją DI apibrėžtį Komisija pateikė komunikate „Dirbtinis intelektas Europai“⁴⁶. Šią apibrėžtį patikslino Aukšto lygio ekspertų grupė⁴⁷.

Bet kuriame naujame teisiniame dokumente DI apibrėžtis turės būti pakankamai lanksti, kad būtų galima atsižvelgti į technikos pažangą, ir kartu pakankamai tiksli, kad būtų užtikrintas būtinas teisinis tikrumas.

Šioje baltojoje knygoje, taip pat turint omeny visas galimas diskusijas dėl politikos iniciatyvų ateityje svarbu paaiškinti pagrindinius DI elementus. Tai „duomenys“ ir „algoritmai“. DI gali būti integruotas į aparatinę įrangą. Vienas iš DI posistemių yra mašinų mokymasis, kai algoritmai mokomi nustatyti tam tikrus dėsningumus iš duomenų rinkinio, pagal kuriuos nustatoma, kokių veiksmų reikia konkrečiam tikslui pasiekti. Algoritmai gali

Pavyzdžiui, savivaldžio automobilio algoritmas naudoja tikrąjį laiko automobilio (greičio, degalų sąnaudų, amortizatorių ir t. t.) ir visą automobilio aplinką (kelį, ženklus, kitas transporto priemones, pėsčiuosius ir t. t.) skenuojančių jutiklių duomenis nustatyti automobilio kryptį, greitėjimui ir greičiui, kad jis pasiektų tam tikrą paskirties vietą. Pagal nustatytus duomenimis algoritmas prisitaiko prie kelio ir išorės sąlygų, taip pat kitų vairuotojų elgesio, užtikrindamas patogiausią ir saugiausią važiavimą.

mokytis ir tada, kai yra naudojami. DI produktai gali veikti savarankiškai, vertindami savo aplinką ir nesivadovaudami iš anksto nustatytomis instrukcijomis, tačiau jų veikimą iš esmės nustato ir apriboja jų kūrėjai. Tikslus, kuriems turėtų būti optimizuota DI sistema, nustato ir programuoja žmogus.

ES yra nustačiusi griežtą teisės aktų sistemą, kuria, *inter alia*, užtikrinama vartotojų apsauga, kovojama su nesąžininga komercine praktika ir apsaugomi asmens duomenys bei privatumas. Be to, *acquis* nustatytos konkrečios taisyklės tam tikriems sektoriams (pvz., sveikatos priežiūros ar transporto). Šios galiojančios ES teisės nuostatos ir toliau bus taikomos dirbtiniam intelektui, nors tam tikrus teisės aktus gali reikėti atnaujinti, kad būtų atsižvelgta į skaitmeninę transformaciją ir DI naudojimą (žr. B skirsnį). Todėl tie aspektai, kurie jau reglamentuojami galiojančiais horizontaliaisiais

⁴⁶ COM(2018) 237 *final*, p. 1: „Dirbtinis intelektas – tai sistemos, kurios elgiasi protingai, analizuodamos savo aplinką ir darydamos gana savarankiškus sprendimus tikslui pasiekti.

Dirbtinio intelekto sistemos gali būti grindžiamos vien tik programine įranga ir veikti virtualiajame pasaulyje (pvz., balso sintezatoriai, vaizdo analizės programinė įranga, paieškos sistemos, kalbos ir veido atpažinimo sistemos) arba gali būti integruotos techninėje įrangoje (pvz., pažangiuose robotuose, [savivaldžiuose automobiliuose], bepiločiuose orlaiviuose ar daiktų interneto objektuose)“.

⁴⁷ Aukšto lygio ekspertų grupės suformuluota DI apibrėžtis (p. 8): „Dirbtinio intelekto (DI) sistemos yra žmonių sukurtos programinės įrangos (taip pat gali būti aparatinės įrangos) sistemos, kurios, joms nustačius sudėtingą tikslą, veikia fiziniu ir skaitmeniniu lygmenimis – įvertina savo aplinką rinkdamos duomenis, aiškina surinktus struktūruotus ir nestruktūruotus duomenis, logiškai analizuoja turimas žinias arba apdoroja pagal tuos duomenis suformuotą informaciją ir priima sprendimą, kokį (-ius) veiksmą (-us) geriausia atlikti, kad užsibrėžtas tikslas būtų pasiektas. DI sistemos gali naudoti simbolines taisykles arba išmoktą skaitmeninį modelį, jos taip pat gali koreguoti savo elgesį analizuodamos, kokį poveikį aplinkai padarė jų ankstesni veiksmai.“

arba sektoriniais teisės aktais (pvz., dėl medicinos priemonių⁴⁸, transporto sistemų), ir toliau bus jais reglamentuojami.

Apskritai naujoji DI reglamentavimo sistema turėtų būti veiksminga, kad būtų pasiekti užsibrėžti tikslai, ir neturėtų būti pernelyg griežta, kad neužkrautų neproporcingos naštos, ypač MVĮ. Siekdamą išlaikyti šią pusiausvyrą, Komisija laikosi nuomonės, kad požiūris turėtų būti grindžiamas rizika.

Tai svarbu siekiant užtikrinti, kad reguliavimo priemonės būtų proporcingos. Tačiau reikalingi aiškūs DI prietaikų diferencijavimo kriterijai, visų pirma norint atsakyti į klausimą, kurios iš jų yra labai rizikingos⁴⁹. Labai rizikingos DI prietaikos apibrėžtis turėtų būti aiški, lengvai suprantama ir taikomas visoms suinteresuotosioms šalims. Net jeigu DI prietaika nelaikoma labai rizikinga, jai vis tiek taikomos jau galiojančios ES taisyklės.

Komisija laikosi nuomonės, kad iš esmės tam tikra DI prietaika turėtų būti laikoma labai rizikinga atsižvelgiant į tai, kuo rizikuojama, įvertinant tai, ar sektorius ir numatyta paskirtis yra susiję su didele rizika, visų pirma ar nepažeidžiama sauga, vartotojų teisės ir pagrindinės teisės. Konkrečiau kalbant, DI prietaika turėtų būti laikoma labai rizikinga, jei atitinka abu kumuliacinius kriterijus:

- pirma, DI prietaika naudojama sektoriuje, kuriame dėl įprastai vykdomos veiklos pobūdžio tikėtina didelė rizika. Pirmasis kriterijus užtikrina, kad reguliavimo priemonės būtų tikslingai taikomos tose srityse, kuriose rizika yra labiausiai tikėtina. Išsamus konkrečių sektorių sąrašas turėtų būti įtrauktas į naują reglamentavimo sistemą. Sektorių pavyzdžiai: sveikatos priežiūra, transportas, energetika ir tam tikros viešojo sektoriaus dalys⁵⁰. Tas sąrašas turėtų būti periodiškai peržiūrimas ir prireikus keičiamas atsižvelgiant į aktualius praktinius pokyčius;
- antra, DI prietaika tam tikrame sektoriuje naudojama taip, kad gali kilti didelė rizika. Šiuo antruoju kriterijumi pripažįstama, kad ne kiekviena DI prietaika tam tikruose sektoriuose būtinai kels didelę riziką. Nors antai sveikatos priežiūra apskritai gali būti svarbus sektorius, klaida registracijos pas gydytojus sistemoje paprastai nesukelia tokio didelio pavojaus, kad dėl to reikėtų imtis teisėkūros veiksmų. Konkretaus naudojimo atvejo rizika galėtų būti vertinama pagal poveikį susijusioms šalims. Pavyzdžiui, DI prietaikų naudojimas, kuris turi teisinį arba panašų didelį poveikį asmens arba įmonės teisėms; dėl kurio kyla sužalojimo, mirties arba didelės turtinės ar neturtinės žalos rizika; dėl kurio atsiranda padarinių, kurių fiziniai ar juridiniai asmenys negali racionaliai išvengti.

Taikant abu kumuliacinius kriterijus būtų užtikrintas tikslingas reglamentavimo sistemos taikymas ir teisinis tikrumas. Iš principo tik pagal abu kumuliacinius kriterijus labai rizikingomis laikomoms prietaikoms būtų taikomi naujojoje DI reglamentavimo sistemoje nustatysimi privalomi reikalavimai (žr. D skirsnį).

Nepaistant to, gali būti ir išimtinių atvejų, kai dėl keliamo pavojaus tam tikroms reikmėms naudojamos DI prietaikos savaime laikytinos labai rizikingomis, tai yra nepriklausomai nuo

⁴⁸ Pavyzdžiui, skiriasi DI sistemų, teikiančių specializuotą medicininę informaciją gydytojams, DI sistemų, teikiančių medicininę informaciją tiesiai pacientui, ir DI sistemų, atliekančių tiesioginius medicininius veiksmus pacientui, saugos aspektai ir teisiniai padariniai. Komisija nagrinėja šiuos sveikatos priežiūrai aktualius saugos ir atsakomybės klausimus.

⁴⁹ ES teisės aktuose, priklausomai nuo srities, pavyzdžiui, gaminių saugos, gali būti skiriamos kitokios rizikos kategorijos nei čia.

⁵⁰ Galėtų būti įtrauktos šios viešojo sektoriaus sritys: prieglobstis, migracija, sienų kontrolė ir teisminės institucijos, socialinė apsauga ir užimtumo tarnybos.

konkreto sektoriaus, ir joms toliau aptariami reikalavimai vis tiek būtų taikomi⁵¹. Iliustratyviai pirmiausia būtų galima paminėti šiuos atvejus:

- Atsižvelgiant į svarbą žmonėms ir į ES *acquis* dėl lygių galimybių įsidarbinti, DI prietaikos, naudojamos įdarbinimo procesuose ir situacijose, kuriose daromas poveikis darbuotojų teisėms, visada būtų laikomos labai rizikingomis, todėl joms visada būtų taikomi toliau aptariami reikalavimai. Dar būtų galima apsvarstyti kitas konkrečias prietaikas, turinčias įtakos vartotojų teisėms.
- DI prietaikos, naudojamos nuotoliniam biometriniam tapatybės nustatymui⁵² ir kitoms intervencinėms sekimo technologijoms, visada būtų laikomos labai rizikingomis, todėl joms visada būtų taikomi toliau aptariami reikalavimai.

D. REIKALAVIMŲ TIPAI

Rengiant būsimą DI reglamentavimo sistemą reikės nuspręsti, kokie privalomieji teisiniai reikalavimai bus taikomi atitinkamiems subjektams. Šie reikalavimai gali būti patikslinti standartais. Kaip nurodyta C skirsnyje, be jau galiojančių teisės aktų, tie reikalavimai būtų taikomi tik labai rizikingoms DI prietaikoms, taip užtikrinant, kad reguliavimo priemonės būtų tikslingos ir proporcingos.

Atsižvelgiant į Aukšto lygio ekspertų grupės gaires ir į tai, kas išdėstyta pirmiau, labai rizikingoms DI prietaikoms taikytinų reikalavimų pagrindiniai aspektai galėtų būti tokie (išsamiau aptariami tolesniuose poskirsiuose):

- mokomieji duomenys;
- duomenų ir įrašų saugojimas;
- teiktina informacija;
- patvarumas ir tikslumas;
- žmogaus atliekama priežiūra;
- konkretūs reikalavimai tam tikroms DI prietaikoms, pavyzdžiui, naudojamoms nuotoliniam biometriniam tapatybės nustatymui.

Siekiant užtikrinti teisinį tikrumą, šie reikalavimai bus tikslinami, kad visiems subjektams, kurie turės jų laikytis, būtų nustatytas aiškus lyginamasis standartas.

a) Mokomieji duomenys

Kaip niekad svarbu propaguoti, stiprinti ir ginti ES vertybes ir taisykles, visų pirma piliečių teises, įtvirtintas ES teisės aktais. Be jokios abejonės, šios pastangos apima ir čia aptariamas labai rizikingas DI prietaikas, kuriomis prekiaujama ir kurios naudojamos ES.

Kaip jau minėta, be duomenų DI neegzistuoja. Daugelio DI sistemų veikimas ir jas naudojant atliekami veiksmai bei priimami sprendimai labai priklauso nuo duomenų rinkinio, naudojamo joms mokytis. Todėl reikėtų imtis būtinų priemonių užtikrinti, kad duomenis naudojant DI sistemoms mokytis

⁵¹ Pažymėtina, kad gali būti taikomi ir kiti ES teisės aktai. Pavyzdžiui, DI prietaikų, integruojamų į vartojimo prekes, saugai gali būti taikoma Direktyva dėl bendros gaminių saugos.

⁵² Nuotolinį biometrinių tapatybės nustatymą reikėtų skirti nuo biometrinio sutikrinimo (pastarasis yra saugumo procedūra, kurią taikant pagal asmens unikalias biologines ypatybes patikrinama, ar asmuo yra tas, kuo teigia esąs). Nuotolinis biometrinis tapatybės nustatymas – nuotoliniu būdu viešoje erdvėje nenutrūkstamai vykdomas daugelio asmenų tapatybės nustatymas pagal biometrinius identifikatorius (pirštų atspaudus, veido atvaizdą, rainelę, kraujagyslių raštą ir kt.) lyginant juos su duomenų bazių duomenimis.

būtų laikomasi ES vertybių ir taisyklių, visų pirma saugos taisyklių ir galiojančiais teisės aktais nustatytų pagrindinių teisių apsaugos taisyklių. DI sistemoms mokytį naudojamų duomenų rinkiniams galėtų būti nustatyti tokie reikalavimai:

- reikalavimai dėl pagrįsto patikinimo, kad paskesnis produktų ar paslaugų, grindžiamų DI sistemomis, naudojimas yra saugus, nes jie atitinka taikytinų (galiojančių ir galimų papildomų) ES saugos taisyklių reikalavimus. Pavyzdžiui, reikalavimai, kuriais užtikrinama, kad DI sistemoms mokytį būtų naudojami duomenų rinkiniai, kurie yra pakankamai platūs ir apima visus scenarijus, kurių reikia siekiant išvengti pavojingų situacijų;
- reikalavimai imtis pagrįstų priemonių siekiant užtikrinti, kad toks paskesnis DI sistemų naudojimas nesukeltų padarinių, susijusių su draudžiama diskriminacija. Šie reikalavimai visų pirma galėtų apimti pareigą naudoti pakankamai reprezentatyvius duomenų rinkinius, ypač siekiant užtikrinti, kad tuose duomenų rinkiniuose būtų tinkamai atspindėti visi reikiami lyties, etninės kilmės ir kitų galimų draudžiamos diskriminacijos priežasčių aspektai;
- reikalavimai, kuriais užtikrinama tinkama privatumo ir asmens duomenų apsauga naudojant DI produktus ir paslaugas. Klausimai, priklausantys Bendrojo duomenų apsaugos reglamento ir Teisės saugos direktyvos taikymo sričiai, šiais teisės aktais ir reglamentuojami.

b) Įrašų ir duomenų saugojimas

Atsižvelgiant į tokias daugelio DI sistemų ypatybes, kaip sudėtingumas ir neskaidrumas, ir dėl jų galinčius kilti sunkumus veiksmingai patikrinti atitiktį taikytinoms taisyklėms ir užtikrinti jų vykdymą, reikia nustatyti įrašų, susijusių su algoritmo programavimu ir labai rizikingoms DI sistemoms mokytį naudojamais duomenimis, saugojimo ir, kai tinkama, pačių duomenų saugojimo reikalavimus. Šie reikalavimai iš esmės leidžia atsekti ir patikrinti DI sistemų veiksmus ar sprendimus, dėl kurių gali kilti problemų. Tai ne tik palengvintų priežiūrą ir vykdymo užtikrinimą, bet ir susiję ekonominės veiklos vykdytojai būtų labiau skatinami anksčiau atkreipti dėmesį į būtinybę laikytis šių taisyklių.

Tuo tikslu reglamentavimo sistemoje galėtų būti nustatyta, kad turėtų būti saugomi:

- tikslūs duomenų rinkinio, naudoto DI sistemoms mokytį ir išbandyti, įrašai, įskaitant pagrindinių charakteristikų ir duomenų rinkinio atrankos aprašymą;
- tam tikrais pagrįstais atvejais – patys duomenų rinkiniai;
- dokumentai, kuriuose išdėstytos programavimo⁵³ ir mokymo metodikos, DI sistemų kūrimo, išbandymo ir validavimo procesai ir metodai, kai aktualu, nurodant, kaip užtikrinta sauga ir išvengta tendencingumo, dėl kurio galėtų atsirasti draudžiama diskriminacija.

Kad būtų užtikrintas veiksmingas atitinkamų teisės aktų vykdymas, įrašai, dokumentai ir, kai aktualu, duomenų rinkiniai turėtų būti saugomi tam tikrą pagrįstos trukmės laikotarpį. Reikėtų nustatyti priemones siekiant užtikrinti, kad pateikus prašymą su jais būtų galima susipažinti, visų pirma kompetentingoms institucijoms bandymams ar patikrinimams atlikti. Prireikus turėtų būti nustatyta konfidencialios informacijos, pavyzdžiui, komercinių paslapčių, apsaugos užtikrinimo tvarka.

c) Informacijos teikimas

⁵³ Pavyzdžiui, dokumentuojamas algoritmas, be kita ko, nurodant, kas turėtų būti optimizuojama modeliu, kokie svoriniai koeficientai iš pradžių numatyti tam tikriems parametrams ir t. t.

Skaidrumas turi būti užtikrinamas ne tik pagal c punkte aptartus įrašų saugojimo reikalavimus. Norint pasiekti užsibrėžtus tikslus, visų pirma propaguoti atsakingą DI naudojimą, stiprinti pasitikėjimą ir prireikus padėti apginti savo teises, svarbu užtikrinti, kad iniciatyviai būtų teikiama tinkama informacija apie labai rizikingų DI sistemų naudojimą.

Tam būtų galima apsvarstyti tokius reikalavimus:

- užtikrinti, kad būtų teikiama aiški informacija apie DI sistemos galimybes ir apribojimus, visų pirma apie jos paskirtį, sąlygas, kuriomis galima tikėtis, kad ji veiks taip, kaip numatyta, ir numatomą tikslumo lygį siekiant konkretaus tikslo. Ši informacija yra ypač svarbi sistemų diegėjams, tačiau ji taip pat gali būti aktuali kompetentingoms institucijoms ir susijusioms šalims;
- be to, piliečiai turėtų būti aiškiai informuojami, kad sąveikauja su DI sistema, o ne su žmogumi. Nors ES duomenų apsaugos teisės aktuose jau yra tam tikrų tokio pobūdžio taisyklių⁵⁴, minėtiems tikslams pasiekti gali reikėti nustatyti papildomus reikalavimus. Jei tai būtų daroma, reikėtų vengti nereikalingos naštos. Todėl tokios informacijos nereikėtų teikti, pavyzdžiui, tais atvejais, kai žmonėms iš karto akivaizdu, kad jie sąveikauja su DI sistemomis. Taip pat svarbu, kad teikiama informacija būtų objektyvi, glausta ir lengvai suprantama. Informacijos teikimo būdas turėtų būti pritaikytas prie konkrečių aplinkybių.

d) Patvarumas ir tikslumas

DI sistemos ir, žinoma, labai rizikingos DI prietaikos, kad būtų patikimos, turi būti techniškai patvarios ir tikslios. Tai reiškia, kad tokios sistemos turi būti kuriamos atsakingai, iš anksto tinkamai apsvarstant, kokią riziką jos gali kelti. DI sistemos turi būti kuriamos ir veikti taip, kad jų veiksmas būtų tokie patikimi, kaip numatyta. Reikėtų imtis visų pagrįstų priemonių, kad būtų kuo labiau sumažinta žalos rizika.

Tam būtų galima apsvarstyti tokius reikalavimus:

- reikalavimai, kuriais užtikrinama, kad visais DI sistemų gyvavimo ciklo etapais jos būtų patvarios ir tikslios arba bent jau atitiktų numatytą tikslumo lygį;
- reikalavimai, kuriais užtikrinamas rezultatų atkuriamumas;
- reikalavimai, kuriais užtikrinama, kad DI sistemos galėtų tinkamai šalinti klaidas ar neatitiktis visais gyvavimo ciklo etapais;
- reikalavimai, kuriais užtikrinama, kad DI sistemos būtų atsparios tiek atviriems išpuoliams, tiek subtilesniems bandymams manipuluoti duomenimis ar pačiais algoritmais, ir kad tokiais atvejais būtų imamasi rizikos mažinimo priemonių.

e) Žmogaus atliekama priežiūra

⁵⁴ Pagal BDAR 13 straipsnio 2 dalies f punktą duomenų valdytojai, gaudami asmens duomenis, duomenų subjektams pateikia kitą būtiną informaciją duomenų tvarkymo sąžiningumui ir skaidrumui užtikrinti, t. y. informuoja apie tai, kad esama automatizuoto sprendimų priėmimo, ir pateikia tam tikrą papildomą informaciją.

Žmogaus atliekama priežiūra padeda užtikrinti, kad DI sistema nesumažintų žmogaus autonomijos ir nesukeltų kitokio neigiamo poveikio. Patikimo, etiško ir į žmogų orientuoto DI tikslą galima pasiekti tik užtikrinant tinkamą žmogaus dalyvavimą kuriant ir naudojant labai rizikingas DI prietaikas.

Nors visos DI prietaikos, kurioms šioje baltojoje knygoje svarstoma taikyti specialią teisinę tvarką, laikomos labai rizikingomis, žmogaus atliekamos priežiūros pobūdis ir laipsnis skirtingais atvejais gali skirtis. Tai visų pirma priklauso nuo numatytos sistemų paskirties ir poveikio, kurį jų naudojimas galėtų turėti susijusiems fiziniams ir juridiniams asmenims. Be to, kai DI sistema tvarko asmens duomenis, neturėtų būti pažeidžiamos BDAR nustatytos juridinės teisės. Pavyzdžiui, žmogaus atliekama priežiūra galėtų būti tokia:

- DI sistemos sprendimai negalioja, kol jų neperžiūrėjo ir nepatvirtino žmogus (pvz., atmesti prašymą skirti socialinę išmoką gali tik žmogus);
- DI sistemos sprendimai galioja iš karto, tačiau žmogaus įsikišimas užtikrinamas vėliau (pvz., DI sistema gali atmesti paraišką išduoti kredito kortelę, tačiau vėliau ją turi galėti peržiūrėti žmogus);
- DI sistemos veikimas stebimas ir yra galimybė įsikišti tikruoju laiku ir ją išjungti (pvz., savivaldyje automobilyje yra mygtukas arba procedūra, kuriais gali pasinaudoti žmogus nustatęs, kad automobilis važiuoja nesaugiai);
- DI sistemos veikimo apribojimai nustatomi projektavimo etapu (pvz., savivaldis automobilis nebevažiuoja tam tikromis prasto matomumo sąlygomis, kai jutikliai mažiau patikimi, arba bet kokiomis sąlygomis turi išlaikyti tam tikrą atstumą nuo prieš jį važiuojančios transporto priemonės).

f) *Specialūs nuotolinio biometrinio tapatybės nustatymo reikalavimai*

Renkant ir naudojant biometrinius duomenis⁵⁵ tapatybei nustatyti nuotoliniu būdu⁵⁶, pvz., diegiant veido atpažinimo technologijas viešose vietose, kyla tam tikra pagrindinių teisių pažeidimo rizika⁵⁷. Nuotolinio biometrinio tapatybės nustatymo DI sistemų naudojimo poveikis pagrindinėms teisėms gali labai skirtis priklausomai nuo jų naudojimo tikslo, aplinkybių ir masto.

⁵⁵ Biometriniai duomenys yra „po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę, kaip antai veido atvaizdai arba daktiloskopiniai [pirštų atspaudų] duomenys“. Teisėsaugos direktyvos 3 straipsnio 13 punktas, BDAR 4 straipsnio 14 punktas, Reglamento (ES) 2018/1725 3 straipsnio 18 punktas.

⁵⁶ Taikant veido atpažinimo technologijas, tapatybė nustatoma asmens veido atvaizdo šabloną lyginant su daug kitų duomenų bazėje saugomų šablonų, siekiant sužinoti, ar joje saugomas tas atvaizdas. Atliekant biometrinį sutikrinimą, priešingai, atvaizdas palyginamas su vienu atvaizdu. Jis leidžia palyginti du biometrinius šablonus, paprastai darant prielaidą, kad jie priklauso tam pačiam asmeniui. Lyginami du biometriniai šablonai siekiant nustatyti, ar abu atvaizdai yra to paties asmens. Tokia procedūra įdiegta, pavyzdžiui, automatizuotos sienų kontrolės vartuose, kurie naudojami oro uostuose patikrinimams kertant sieną atlikti.

⁵⁷ Pavyzdžiui, žmogaus teisės į orumą. Didžiausią susirūpinimą, susijusį su pagrindinėmis teisėmis, naudojant veido atpažinimo technologijas kelia teisės į privatų gyvenimą ir asmens duomenų apsaugą pažeidimai. Taip pat gali būti daromas poveikis tam tikrų grupių, pavyzdžiui, vaikų, vyresnio amžiaus asmenų ir neįgaliųjų, nediskriminavimui ir teisėms. Naudojant šią technologiją neturi būti pažeidžiama ir teisė į saviraiškos, asociacijų ir susirinkimų laisvę. Daugiau žr. *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, <https://fra.europa.eu/en/publication/2019/facial-recognition>.

ES duomenų apsaugos taisyklėmis iš esmės draudžiama tvarkyti biometrinius duomenis siekiant konkrečiai nustatyti fizinio asmens tapatybę, išskyrus atvejus, kai tenkinamos specialios sąlygos⁵⁸. Pagal BDAR toks duomenų tvarkymas gali būti atliekamas tik dėl kelių priežasčių, o pagrindinė iš jų – svarbus viešasis interesas. Tokiu atveju duomenys turi būti tvarkomi pagal ES arba nacionalinę teisę, laikantis proporcingumo reikalavimų, nepažeidžiant esminių teisės į duomenų apsaugą nuostatų ir užtikrinant tinkamas apsaugos priemones. Pagal Teisėsaugos direktyvą toks duomenų tvarkymas turi būti tikrai būtinas, iš esmės leidžiamas pagal ES arba nacionalinę teisę ir atliekamas taikant tinkamas apsaugos priemones. Kadangi bet koks biometrinių duomenų tvarkymas siekiant konkrečiai nustatyti fizinio asmens tapatybę yra ES teisėje nustatyto draudimo išimtis, jam būtų taikoma ES pagrindinių teisių chartija.

Vadinasi, pagal galiojančias ES duomenų apsaugos taisykles ir Pagrindinių teisių chartiją DI gali būti naudojamas nuotoliniam biometriniam tapatybės nustatymui tik tais atvejais, kai toks naudojimas yra tinkamai pagrįstas, proporcingas ir jam taikomos tinkamos apsaugos priemonės.

Siekdama išsklaidyti dėl tokio DI naudojimo viešose vietose galintį kilti visuomenės nerimą ir išvengti vidaus rinkos susiskaidymo, Komisija pradės plačias Europos masto diskusijas dėl aplinkybių, jei tokių yra, kuriomis būtų pateisinamas toks naudojimas, ir dėl bendrų apsaugos priemonių.

E. ADRESATAI

Kalbant apie subjektus, kuriems būtų taikomi su pirmiau aptartomis labai rizikingomis DI prietaikomis susiję teisiniai reikalavimai, reikia apsvarstyti du pagrindinius klausimus.

Pirmas klausimas – kaip pareigos turi būti paskirstytos susijusiems ekonominės veiklos vykdytojams. Į DI sistemos gyvavimo ciklą įsitraukia daug subjektų. Tai kūrėjas, diegėjas (asmuo, kuris naudoja DI produktą ar paslaugą) ir kiti potencialūs asmenys (gamintojas, platintojas ar importuotojas, paslaugų teikėjas, profesionalus ar privatus naudotojas).

Komisijos nuomone, būsimoje reglamentavimo sistemoje kiekvienas įpareigojimas turėtų būti skirtas tam subjektui (-ams), kuris gali geriausiai sumažinti galimą riziką. Pavyzdžiui, DI kūrėjai gali geriausiai spręsti su kūrimo etapu susijusios rizikos klausimą, bet jų galimybės valdyti riziką naudojimo etapu gali būti labiau ribotos. Tokiu atveju atitinkamas įpareigojimas turėtų būti taikomas diegėjui. Tai neturi įtakos klausimui, kuri šalis, siekiant užtikrinti atsakomybę galutiniams naudotojams ar kitoms nukentėjusioms šalims ir veiksmingą teisę kreiptis į teismą, turėtų būti atsakinga už padarytą žalą. Pagal ES atsakomybės už gaminius teisę už gaminius su trūkumais atsakingas gamintojas; tai neprieštarauja tam, kad pagal nacionalinės teisės aktus taip pat gali būti leidžiama išieškoti žalą iš kitų šalių.

Antras klausimas kyla dėl teisėkūros priemonių geografinės taikymo srities. Komisijos nuomone, labai svarbu, kad reikalavimai būtų taikomi visiems DI produktams ar paslaugoms Europos Sąjungoje siūlantiesiems ekonominės veiklos vykdytojams, neatsižvelgiant į tai, ar jie įsisteigę ES, ar ne. Priešingu atveju nebūtų įmanoma visiškai įgyvendinti pirmiau minėtų teisėkūros priemonių tikslų.

F. REIKALAVIMŲ LAIKYMASIS IR VYKDYMO UŽTIKRINIMAS

Siekiant užtikrinti, kad DI būtų patikimas, saugus ir atitiktų Europos vertybes ir taisykles, turi būti praktiškai laikomasi taikomų teisinių reikalavimų ir jų vykdymą turi veiksmingai užtikrinti tiek

⁵⁸ BDAR 9 straipsnis, Teisėsaugos direktyvos 10 straipsnis. Taip pat žr. Reglamento (ES) 2018/1725 (taikomo ES institucijoms ir įstaigoms) 10 straipsnį.

kompetentingos nacionalinės ir Europos institucijos, tiek susijusios šalys. Kompetentingos institucijos turėtų galėti ne tik tirti atskirus atvejus, bet ir įvertinti poveikį visuomenei.

Atsižvelgdama į didelę tam tikrų DI prietaikų piliečiams ir visai mūsų visuomenei keliamą riziką (žr. A skirsnį), Komisija šiuo etapu mano, kad norint patikrinti ir užtikrinti labai rizikingų DI prietaikų atitiktį tam tikriems iš pirmiau minėtų privalomų reikalavimų (žr. D skirsnį) turėtų būti atliekamas objektyvus išankstinis atitikties vertinimas. Išankstinis atitikties vertinimas galėtų apimti bandymų, tikrinimo ir sertifikavimo procedūras⁵⁹. Galėtų būti tikrinami algoritmai ir duomenų rinkiniai, naudojami kūrimo etapu.

Labai rizikingų DI prietaikų atitikties vertinimas turėtų būti įtrauktas į atitikties vertinimo mechanizmus, kurie jau taikomi daugeliui ES vidaus rinkai pateikiamų gaminių. Tais atvejais, kai tokių mechanizmų nėra, gali reikėti sukurti panašius mechanizmus, remiantis geriausia patirtimi ir galimu suinteresuotųjų subjektų bei Europos standartizacijos organizacijų indėliu. Bet koks toks naujas mechanizmas turėtų būti proporcingas ir nediskriminacinis, turėtų būti taikomi skaidrūs ir objektyvūs kriterijai, atitinkantys tarptautinius įsipareigojimus.

Kuriant ir įgyvendinant išankstinį atitikties vertinimą grindžiamą sistemą visų pirma reikėtų atsižvelgti į šiuos dalykus:

- ne visus pirmiau nurodytus reikalavimus gali būti įmanoma patikrinti per išankstinį atitikties vertinimą. Pavyzdžiui, atliekant tokį vertinimą paprastai negali būti gerai patikrinta atitiktis reikalavimui dėl teiktinos informacijos;
- ypač reikėtų atsižvelgti į tai, kad tam tikros DI sistemos gali evoliucionuoti ir mokytis iš patirties ir todėl tokių DI sistemų atitiktį per gyvavimo laikotarpį gali reikėti įvertinti pakartotinai;
- būtina patikrinti naudotus mokomuosius duomenis ir programavimo bei mokymo metodikas, DI sistemų kūrimo, išbandymo ir validavimo procesus ir metodus;
- jei vertinant atitiktį nustatoma, kad DI sistema neatitinka reikalavimų, pavyzdžiui, susijusių su jai mokytis naudojamais duomenimis, nustatytus trūkumus reikės pašalinti, pavyzdžiui, Europos Sąjungoje sistemą iš naujo apmokyti taip, kad būtų užtikrinta atitiktis visiems taikomiems reikalavimams.

Atitikties vertinimas būtų privalomas visiems ekonominės veiklos vykdytojams, kuriems taikomi reikalavimai, neatsižvelgiant į jų įsisteigimo vietą⁶⁰. Siekiant sumažinti našą MVL, gali būti numatyta tam tikra paramos struktūra, be kita ko, pasitelkiant skaitmeninių inovacijų centrus. Be to, užtikrinti atitiktį galėtų padėti standartai ir specialios internetinės priemonės.

Bet koks išankstinis atitikties vertinimas neturėtų daryti poveikio kompetentingų nacionalinių institucijų atliekamai atitikties stebėsenai ir *ex post* vykdymo užtikrinimui. Tai pasakytina ne tik apie labai rizikingas DI prietaikas, bet ir apie kitas DI prietaikas, kurioms taikomi teisiniai reikalavimai, tačiau dėl aptariamų prietaikų rizikingumo kompetentingos nacionalinės valdžios institucijos gali skirti ypatingą dėmesį pirmosioms. Atlikti *ex post* patikras turėtų padėti tinkama atitinkamos DI prietaikos

⁵⁹ Sistema būtų grindžiama ES atitikties vertinimo procedūromis, žr. Sprendimą 768/2008/EB arba Reglamentą (ES) 2019/881 (Kibernetinio saugumo aktą), atsižvelgiant į DI specifiką. Žr. Mėlynąjį vadovą dėl gaminius reglamentuojančių ES taisyklių įgyvendinimo, 2014 m.

⁶⁰ Dėl susijusios valdymo struktūros, įskaitant įstaigas, paskirtas atlikti atitikties vertinimą, žr. H skirsnį.

dokumentacija (žr. E skirsnį) ir prireikus galimybė trečiosioms šalims, pavyzdžiui, kompetentingoms institucijoms, išbandyti tokias prietaikas. Tai gali būti ypač svarbu, kai tam tikromis aplinkybėmis kyla pavojus pagrindinėms teisėms. Atitiktis stebėsenai turėtų būti įtraukta į nuolatinės rinkos priežiūros sistemą. Valdymo aspektai aptariami H skirsnyje.

Be to, šalims, kurioms DI sistemos – tiek labai rizikingos DI prietaikos, tiek kitos DI prietaikos – padarė neigiamą poveikį, turėtų būti užtikrinta teisė į veiksmingas teismines priemones. Atsakomybės klausimai išsamiau aptariami kartu su šia baltąja knyga skelbiamoje ataskaitoje dėl saugos ir atsakomybės teisės aktų.

G. SAVANORIŠKAS NERIZIKINGŲ DI PRIETAIKŲ ŽENKLINIMAS

DI prietaikoms, kurios nelaikomos rizikingomis (žr. C skirsnį) ir kurioms dėl to netaikomi pirmiau aptarti privalomi reikalavimai (žr. D, E ir F skirsnius), būtų galima, be taikytinų teisės aktų, nustatyti savanoriško ženklavimo sistemą.

Taikant tą sistemą, suinteresuoti ekonominės veiklos vykdytojai, kuriems netaikomi privalomi reikalavimai, galėtų savanoriškai taikyti arba tuos privalomus reikalavimus, arba savanoriško ženklavimo sistemos taikymo tikslais specialiai nustatytus panašius reikalavimus. Tokių ekonominės veiklos vykdytojų DI prietaikoms būtų suteiktas kokybės ženklas.

Savanorišką ženklavimą pasirinkę ekonominės veiklos vykdytojai parodytų, kad jų DI produktai ir paslaugos yra patikimi, o naudotojai lengvai atpažintų, kad tokie produktai ir paslaugos atitinka tam tikrus objektyvius ir standartizuotus europinius lyginamuosius etalonus, viršijančius įprastai taikomus teisinius įpareigojimus. Tai padėtų padidinti naudotojų pasitikėjimą DI sistemomis ir apskritai skatintų labiau jas naudoti.

Pasirinkus šią galimybę būtų sukurta nauja teisinė priemonė, kuria būtų nustatyta savanoriško ženklavimo sistema rizikingomis nelaikytinų DI sistemų kūrėjams ir (arba) diegėjams. Nors dalyvavimas ženklavimo sistemoje būtų savanoriškas, kūrėjui ar diegėjui nusprendus naudoti ženklą, reikalavimai būtų privalomi. Kad būtų užtikrinta atitiktis visiems reikalavimams, turėtų būti derinamas *ex ante* ir *ex post* vykdymo užtikrinimas.

H. VALDYMAS

Europinė DI valdymo struktūra, kuri būtų nacionalinių kompetentingų institucijų bendradarbiavimo platforma, yra reikalinga siekiant išvengti atsakomybės fragmentacijos, didinti valstybių narių pajėgumus ir užtikrinti, kad Europa ilgainiui įgytų pajėgumų DI produktams ir paslaugoms išbandyti ir sertifikuoti. Atsižvelgiant į tai, būtų svarbu remti kompetentingas nacionalines institucijas, kad jos galėtų vykdyti savo įgaliojimus ten, kur DI naudojamas.

Europinės valdymo struktūros užduotys galėtų būti įvairios: tai galėtų būti forumas, kuriame reguliariai keičiamasi informacija ir geriausia patirtimi, nustatomos besiformuojančios tendencijos, patariama standartizavimo ir sertifikavimo klausimais. Ji taip pat turėtų didelę reikšmę teisės aktų sistemos įgyvendinimo palengvinimui, pavyzdžiui, būtų teikiamos gairės, nuomonės ir dalykinės žinios. Šiuo tikslu ji turėtų remtis nacionalinių valdžios institucijų tinklu, taip pat sektoriais tinklais ir reguliavimo institucijomis nacionaliniu ir ES lygmenimis. Be to, Komisijai galėtų padėti ekspertų komitetas.

Valdymo struktūra turėtų užtikrinti kuo aktyvesnį suinteresuotųjų subjektų dalyvavimą. Su suinteresuotaisiais subjektais – vartotojų organizacijomis ir socialiniais partneriais, įmonėmis,

mokslininkais, pilietinės visuomenės organizacijomis – turėtų būti konsultuojamasi dėl teisės aktų sistemos įgyvendinimo ir tobulinimo.

Siūloma valdymo struktūra neturėtų dubliuoti jau egzistuojančių struktūrų, pavyzdžiui, finansų, farmacijos, aviacijos, medicinos priemonių, vartotojų apsaugos, duomenų apsaugos srityse, funkcijų. Vietoj to ji turėtų užmegzti glaudžius ryšius su kitomis įvairių sektorių ES ir nacionalinėmis kompetentingomis institucijomis, kad papildytų turimas ekspertines žinias ir padėtų joms stebėti ir prižiūrėti ekonominės veiklos vykdytojų veiklą, susijusią su DI sistemomis ir DI produktais bei paslaugomis.

Galiausiai, pasirinkus šią galimybę, atitikties vertinimą būtų galima patikėti valstybių narių paskirtoms notifikuotosioms įstaigoms. Nepriklausomą DI sistemų auditą ir vertinimą pagal pirmiau išdėstytus reikalavimus būtų galima atlikti bandymų centruose Nepriklausomas vertinimas didins pasitikėjimą ir užtikrins objektyvumą. Jis taip pat galėtų palengvinti susijusių kompetentingų institucijų darbą.

ES turi puikių bandymų ir vertinimo centrų ir turėtų didinti savo pajėgumus ir DI srityje. Ekonominės veiklos vykdytojai, įsisteigę trečiosiose valstybėse, norintys patekti į vidaus rinką, galėtų naudotis arba ES įsisteigusių paskirtųjų įstaigų paslaugomis, arba, jeigu sudaryti tarpusavio pripažinimo susitarimai su trečiosiomis šalimis, naudotis trečiųjų šalių įstaigų, paskirtų atlikti tokį vertinimą, paslaugomis.

Šioje baltąjoje knygoje aptariama valdymo struktūra, susijusi su DI ir galimais atitikties vertinimais, nedarytų poveikio už konkrečius sektorius arba konkrečius klausimus (finansų, farmacijos, aviacijos, medicinos priemonių, vartotojų apsaugos, duomenų apsaugos ir kt.) atsakingų kompetentingų institucijų įgaliojimams ir atsakomybei pagal galiojančią ES teisę.

6. IŠVADA

DI – strateginė technologija, kuri yra labai naudinga piliečiams, įmonėms ir visai visuomenei, jeigu ji yra orientuota į žmogų, etiška, tvari ir paiso pagrindinių teisių ir vertybių. DI labai padidina veiksmingumą ir našumą, o tai savo ruožtu gali padidinti Europos pramonės konkurencingumą ir piliečių gerovę. Jis taip pat gali padėti spręsti kai kurias opiausias visuomenės problemas, taip pat padėti kovoti su klimato kaita ir aplinkos būklės blogėjimu, spręsti tvarumo ir demografijos problemas, apsaugoti mūsų demokratiją ir, kai būtina ir proporcinga, kovoti su nusikalstamumu.

Kad Europa galėtų visapusiškai pasinaudoti DI teikiamomis galimybėmis, reikia plėtoti ir stiprinti reikiamus pramoninius ir technologinius pajėgumus. Kaip nurodyta kartu skelbiamoje Europos duomenų strategijoje, tam taip pat reikia priemonių, kurios sudarytų sąlygas ES tapti pasauliniu duomenų centru.

Formuojant Europos požiūrį į DI siekiama skatinti Europos pajėgumą kurti DI inovacijas ir kartu remti etiško ir patikimo DI plėtotę ir diegimą visoje ES ekonomikoje. DI turėtų būti naudingas žmonėms ir užtikrinti visuomenės gerovę.

Šia baltąja knyga ir kartu su ja skelbiama ataskaita dėl saugos ir atsakomybės teisės aktų Komisija pradeda plataus masto konsultacijas su valstybių narių pilietine visuomene, pramone ir akademine bendruomene dėl konkrečių pasiūlymų, susijusių su Europos požiūriu į DI. Jie apima tiek politikos priemones, kuriomis siekiama skatinti investicijas į mokslinius tyrimus ir inovacijas, gerinti įgūdžių ugdymą ir remti MVĮ, kad jos labiau naudotų DI, tiek pasiūlymus dėl pagrindinių būsimos reglamentavimo sistemos elementų. Šios konsultacijos sudarys sąlygas išsamiam dialogui su visomis suinteresuotomis šalimis, kuriuo Komisija remsis imdamasi tolesnių veiksmų.

Komisija ragina teikti pastabas dėl baltojoje knygoje išdėstytų pasiūlymų dalyvaujant tuo tikslu rengiamose viešose konsultacijose adresu https://ec.europa.eu/info/consultations_lt. Pastabas galima teikti iki 2020 m. gegužės 19 d.

Pagal įprastą tvarką Komisija skelbia viešų konsultacijų atsakymus. Tačiau galima reikalauti, kad pateikta informacija ar jos dalys liktų konfidencialios. Tokiu atveju ant pirmojo pateikiamos informacijos puslapio aiškiai nurodykite, kad informacija viešai neskelbtina, ir Komisijai atsiųskite nekonfidencialią pateiktos informacijos versiją, kurią būtų galima paskelbti.