



Briuselis, 2020 02 19
COM(2020) 64 final

**KOMISIJOS ATASKAITA EUROPOS PARLAMENTUI, TARYBAI IR EUROPOS
EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI**

**Ataskaita dėl dirbtinio intelekto, daiktų interneto ir robotikos poveikio saugai ir
atsakomybei**

ATASKAITA DĖL DIRBTINIO INTELEKTO, DAIKTŲ INTERNETO IR ROBOTIKOS POVEIKIO SAUGAI IR ATSAKOMYBEI

1. Įvadas

Dirbtinis intelektas¹, daiktų internetas² ir robotika suteiks mūsų visuomenei naujų galimybių ir naudos. Komisija pripažįsta šių technologijų svarbą bei potencialą ir tai, kad šiose srityse reikia didelių investicijų³. Ji yra įsipareigojusi siekti, kad dirbtinio intelekto, daiktų interneto ir robotikos srityse Europa pirmautų pasaulyje. Šiam tikslui pasiekti reikia aiškos ir nuspėjamos teisinės sistemos, kurioje atsižvelgiama į technologijų keliamas problemas.

1.1. Esama saugos ir atsakomybės sistema

Bendras saugos ir atsakomybės teisinių sistemų tikslas – užtikrinti, kad visi produktai ir paslaugos, įskaitant tuos, į kuriuos diegiamos besiformuojančios skaitmeninės technologijos, būtų saugūs, patikimi ir veiktų darniai ir kad padaryta žala būtų efektyviai ištaisoma. Aukštas produktų ir sistemų, į kuriuos įdiegtos naujos skaitmeninės technologijos, saugos lygis ir patikimi žalos atlyginimo mechanizmai (t. y. atsakomybės sistema) padeda geriau apsaugoti vartotojus. Nuo minėtų dalykų priklauso ir pasitikėjimas šiomis technologijomis – jis būtinas norint, kad jas įsisavintų pramonės subjektai ir naudotojai. Tai padidins mūsų pramonės konkurencingumą ir padės siekti Sąjungos tikslų⁴. Formuojantis naujoms technologijoms, tokioms kaip dirbtinis intelektas, daiktų internetas ir robotika, labai svarbu nustatyti aiškią saugos ir atsakomybės sistemą, kuria būtų galima užtikrinti vartotojų apsaugą ir suteikti teisinį tikrumą įmonėms.

Sąjunga taiko tvirtą ir patikimą saugos ir atsakomybės už gaminius reglamentavimo sistemą ir turi patikimą saugos standartų bazę. Jas papildo atskiri atsakomybę reglamentuojantys nacionalinės teisės aktai. Visa tai drauge užtikrina mūsų piliečių gerovę bendrojoje rinkoje ir skatina inovacijas bei technologijų įsisavinimą. Tačiau dėl dirbtinio intelekto, daiktų interneto ir robotikos keičiasi daugelio produktų ir paslaugų savybės.

2018 m. balandžio 25 d. priimtame komunikate „Dirbtinis intelektas Europai“⁵ paskelbta, kad Komisija pateiks ataskaitą, kurioje įvertins besiformuojančių skaitmeninių technologijų poveikį esamoms saugos ir atsakomybės sistemoms. Šioje ataskaitoje siekiama nustatyti ir išnagrinėti platesnį dirbtinio intelekto, daiktų interneto ir robotikos poveikį atsakomybės ir saugos sistemoms, taip pat galimas tų sistemų spragas. Gairės, pateiktos šioje prie Baltosios knygos dėl dirbtinio intelekto pridėamoje ataskaitoje, yra skirtos diskusijoms ir dėl jų bus plačiau konsultuojamasi su suinteresuotaisiais subjektais. Ataskaitos skirsnis, kuriame

¹ Aukšto lygio ekspertų grupės nustatyta dirbtinio intelekto apibrėžtis pateikta <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>.

² Daiktų interneto apibrėžtis pateikta Rekomendacijoje ITU-T Y.2060 adresu <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>.

³ SWD(2016) 110, COM(2017) 9, COM(2018) 237 ir COM(2018) 795.

⁴ http://ec.europa.eu/growth/industry/policy_lt

⁵ <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=COM%3A2018%3A237%3AFIN>.

Prie komunikato pridėta Komisijos tarnybų darbiname dokumente (2018) 137 (<https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137>) pateikta pirmoji su atsakomybe susijusių problemų, kurias kelia besiformuojančios skaitmeninės technologijos, apžvalga.

nagrinėjami saugos aspektai, grindžiamas Mašinų direktyvos⁶ vertinimu⁷ ir darbo su atitinkamomis ekspertų grupėmis rezultatais⁸. Skirsnis, kuriame nagrinėjami atsakomybės aspektai, grindžiamas Atsakomybės už gaminius direktyvos⁹ vertinimu¹⁰, atitinkamų ekspertų grupių indėliu¹¹ ir bendravimu su suinteresuotaisiais subjektais. Šioje ataskaitoje siekiama ne išsamiai apžvelgti galiojančias saugos ir atsakomybės taisykles, o sutelkti dėmesį į pagrindines iki šiol nustatytas problemas.

1.2. Dirbtinio intelekto, daiktų interneto ir robotikos technologijų savybės

Dirbtinis intelektas, daiktų internetas ir robotika turi daug bendrų savybių. Dėl savo **sąsajumo, autonomiškumo ir priklausomybės nuo duomenų** šios technologijos gali atlikti užduotis beveik ar visiškai nekontroliuojamos arba neprižiūrimos žmogaus. Dirbtiniu intelektu grindžiamos sistemos savo rezultatus gali gerinti mokydamosi iš patirties. Šios technologijos yra **sudėtingos** – tai rodo tiek **tiesimo grandinėje** dalyvaujančių ekonominės veiklos vykdytojų gausa, tiek komponentų, dalių, programinės įrangos, sistemų ar paslaugų (visi šie dalykai drauge sudaro naujas technologijų ekosistemas) įvairovė. Prie šių savybių reikėtų pridėti ir tai, kad rinkai pateiktos technologijos yra **atviros** naujinimui ir naujoviniui. Šioms technologijoms reikia didžiulio kiekio duomenų, jos yra priklausomos nuo algoritmų, o dirbtinio intelekto sprendimų priėmimo procesas yra **neskaidrus** – dėl to dar sunkiau numatyti dirbtiniu intelektu grindžiamo produkto elgseną ir suvokti galimas žalos priežastis. Galiausiai, dirbtinio intelekto ir daiktų interneto produktai dėl savo sąsajumo ir atvirumo gali būti neatsparūs **kibernetinėms grėsmėms**.

1.3. Dirbtinio intelekto, daiktų interneto ir robotikos teikiamos galimybės

Didėjantis naudotojų pasitikėjimas besiformuojančiomis technologijomis ir visuomenės pritarimas joms, tobulesni produktai, procesai bei verslo modeliai ir didesnis Europos gamintojų produktyvumas – tai vos kelios dirbtinio intelekto, daiktų interneto ir robotikos teikiamos galimybės.

Dirbtinis intelektas ne tik padeda didinti produktyvumą ir našumą, bet ir leidžia žmonėms siekti dar neišnaudotų intelektinių galimybių, sudaro sąlygas naujiems atradimams ir padeda spręsti vienus iš didžiausių pasaulio iššūkių: ne tik gydyti lėtines ligas, numatyti ligų

⁶ Direktyva 2006/42/EB.

⁷ SWD(2018) 161 *final*.

⁸ Pagal Direktyvą 2001/95/EB dėl bendros gaminių saugos (BGSD) įsteigtu Vartotojų saugos tinklu ir pagal Mašinų direktyvą 2006/42/EB ir Radijo įrenginių direktyvą 2014/53/ES įsteigtomis ekspertų grupėmis, kurias sudaro valstybių narių atstovai, pramonės subjektai ir kiti suinteresuotieji subjektai, pavyzdžiui, vartotojų asociacijos.

⁹ Direktyva 85/374/EEB.

¹⁰ COM(2018) 246 *final*.

¹¹ Buvo įkurta Atsakomybės ir naujų technologijų ekspertų grupė, kurios tikslas – teikti Komisijai ekspertinių žinių apie Atsakomybės už gaminius direktyvos ir nacionalinių civilinės atsakomybės taisyklių taikymą ir padėti parengti pagrindinius principus, kuriais vadovaujantis bus galima taikomus teisės aktus pritaikyti prie naujų technologijų keliamų iššūkių. Ši grupė yra dvejopos sudėties – viena sprendžia atsakomybės už produktus, kita – su naujomis technologijomis susijusius klausimus (žr. <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1>).

Už naujų technologijų klausimus atsakingos grupės ataskaita „Atsakomybė už dirbtinį intelektą ir kitas besiformuojančias technologijas“ paskelbta https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

protrūkius, mažinti mirčių dėl eismo įvykių skaičių, bet ir kovoti su klimato kaita ar numatyti kibernetines grėsmes.

Šios technologijos gali būti labai naudingos – jos gali pagerinti produktų saugą, kad jie taptų atsparesni tam tikrai rizikai. Pavyzdžiui, dauguma kelių eismo įvykių šiuo metu įvyksta dėl žmogaus klaidų¹², todėl susietosios ir automatizuotos transporto priemonės galėtų padidinti kelių eismo saugumą. Be to, daiktų interneto sistemos gali priimti ir apdoroti didžiulius iš įvairių šaltinių gaunamų duomenų kiekius. Tokį didelį informacijos kiekį galima panaudoti tam, kad juo remdamiesi produktai galėtų patys prisitaikyti ir atitinkamai taptų saugesni. Naudojantis naujomis technologijomis būtų galima veiksmingiau atšaukti produktus iš rinkos, nes, pavyzdžiui, jie patys galėtų įspėti naudotojus vengti saugos problemų¹³. Jei naudojant susietąjį produktą kiltų saugos problemų, gamintojai galėtų tiesiogiai bendrauti su naudotojais: viena vertus, įspėtų juos apie riziką, kita vertus, jei įmanoma, tiesiogiai išspręstų problemą, pavyzdžiui, įdiegtų su sauga susijusį naujinį. Pavyzdžiui, 2017 m. norėdamas atšaukti iš rinkos vieną iš savo prietaisų, išmaniųjų telefonų gamintojas atnaujino programinę įrangą ir atšaukiamų telefonų akumuliatorių talpą sumažino iki nulio¹⁴, kad naudotojai tų pavojingų prietaisų nebenaudotų.

Be to, naujos technologijos gali padėti pagerinti produktų atsekamumą. Pavyzdžiui, naudodamosi daiktų interneto sąsajumu, įmonės ir rinkos priežiūros institucijos galėtų atsekti pavojingus produktus ir nustatyti tiekimo grandinėse kylančią riziką¹⁵.

Tačiau dirbtinis intelektas, daiktų internetas ir robotika ekonomikai ir mūsų visuomenei teikia ne tik galimybių – jie taip pat gali kelti pavojų teisėtiems (tiek materialiniams, tiek nematerialiniams) interesams. Plečiantis prietaikų sričiai tokios žalos rizika didės. Todėl labai svarbu įvertinti, ar dabartinė teisinė saugos ir atsakomybės sistema vis dar yra tinkama naudotojams apsaugoti ir kiek ji tam yra tinkama.

2. Sauga

Komisijos komunikate „Pasitikėjimo į žmogų orientuotu dirbtiniu intelektu didinimas“ teigiama, kad **„į projektuojamas dirbtinio intelekto sistemas turėtų būti integruoti saugos ir saugumo užtikrinimo mechanizmai, kad jos būtų užtikrintai saugios visais etapais, itin daug dėmesio skiriant visų susijusių subjektų fiziniam ir psichiniam saugumui“**¹⁶.

Šiame skirsnyje vertinami Sąjungos gaminių saugos teisės aktai – analizuojama, ar dabartinėje Sąjungos teisės aktų sistemoje yra tinkamų nuostatų, kuriomis užtikrinama, kad į besiformuojančias technologijas ir visų pirma dirbtinio intelekto sistemas būtų įdiegti saugos ir saugumo užtikrinimo mechanizmai.

¹² Apskaičiuota, kad apie 90 proc. kelių eismo įvykių įvyksta dėl žmogaus kaltės. Žr. Komisijos ataskaitą „Automobilių saugos didinimas ES siekiant išsaugoti gyvybes“ (COM(2016) 0787 final).

¹³ Pavyzdžiui, automobilio vairuotoją galima įspėti, kad jis sumažintų greitį, jei kelyje įvyko avarija.

¹⁴ EBPO (2018 m.) *Measuring and maximising the impact of product recalls globally: OECD workshop report* („Produktų atšaukimo poveikio vertinimas ir didinimas pasaulyje. EBPO praktinio seminaro ataskaita“), *OECD Science, Technology and Industry Policy Papers Nr. 56*, OECD Publishing, Paryžius, <https://doi.org/10.1787/ab757416-en>.

¹⁵ EBPO (2018 m.) *Enhancing product recall effectiveness globally: OECD background report* („Produktų atšaukimo veiksmingumo didinimas pasaulyje. EBPO bendroji ataskaita“), *OECD Science, Technology and Industry Policy Papers Nr. 58*, OECD Publishing, Paryžius, <https://doi.org/10.1787/ef71935c-en>.

¹⁶ Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Pasitikėjimo į žmogų orientuotu dirbtiniu intelektu didinimas“, Briuselis, 2019 4 8, COM(2019) 168 final.

Šioje ataskaitoje daugiausia nagrinėjama Direktyva dėl bendros gaminių saugos¹⁷ ir suderinti gaminius reglamentuojantys teisės aktai, atitinkantys horizontaliąsias naujojo požiūrio¹⁸ ir (arba) naujosios teisės aktų sistemos (toliau – Sąjungos gaminių saugos teisės aktai arba sistema)¹⁹ taisykles. Horizontaliosiomis taisyklėmis užtikrinamas atskiruose sektoriuose taikomų gaminių saugos taisyklių nuoseklumas.

Sąjungos gaminių saugos teisės aktais siekiama užtikrinti, kad Sąjungos rinkai tiekiami gaminiai atitiktų griežtus sveikatos, saugos ir aplinkosaugos reikalavimus ir kad tokie gaminiai galėtų laisvai judėti visoje Sąjungoje. Sektorių teisės aktus²⁰ papildė Direktyva dėl bendros gaminių saugos²¹, kurioje reikalaujama, kad visi vartotojams skirti gaminiai, net jei jie neregamentuojami Sąjungos sektorių teisės aktais, būtų saugūs. Saugos taisyklės papildė rinkos priežiūros mechanizmai ir nacionalinėms institucijoms pagal Rinkos priežiūros reglamentą²² ir Direktyvą dėl bendros gaminių saugos²³ suteikti įgaliojimai. Transporto srityje taikomos papildomos Sąjungos ir nacionalinės taisyklės, kurių turi būti laikomasi pradedant eksploatuoti motorinę transporto priemonę²⁴, orlaivį arba laivą, taip pat aiškios taisyklės, kuriomis reglamentuojama sauga jų eksploatavimo metu, įskaitant veiklos vykdytojų uždavinius ir valdžios institucijų vykdomas priežiūros užduotis.

Kitas esminis Sąjungos gaminių saugos teisės aktų elementas – Europos standartizacijos sistema. Atsižvelgiant į visuotinį skaitmeninimo ir besiformuojančių skaitmeninių technologijų pobūdį, tarptautinis bendradarbiavimas standartizacijos srityje yra ypač svarbus Europos pramonės konkurencingumui.

Dauguma Sąjungos gaminių saugos sistemos nuostatų buvo parengta prieš atsirandant tokioms skaitmeninėms technologijoms kaip dirbtinis intelektas, daiktų internetas ar robotika. Todėl toje sistemoje ne visuomet yra nuostatų, kuriomis išsamiai sprendžiamos naujos šių besiformuojančių technologijų keliamos problemos ir mažinama su jomis susijusi rizika. Nors dabartinė gaminių saugos sistema technologijų atžvilgiu yra neutrali, tai nereiškia, kad ji netaikoma produktams, kuriuose yra šių technologijų. Be to, vėlesniuose tos sistemos teisės aktuose, pavyzdžiui, medicinos priemonių ar automobilių sektorių teisės aktuose, jau išsamiai atsižvelgta į kai kuriuos su skaitmeninių technologijų atsiradimu susijusius aspektus, pavyzdžiui, automatizuotus sprendimus, autonominę programinę įrangą ir sąsają.

¹⁷ 2001 m. gruodžio 3 d. Europos Parlamento ir Tarybos direktyva 2001/95/EB dėl bendros gaminių saugos (OL L 11, 2002 1 15, p. 4–17).

¹⁸ OL C 136, 1985 6 4, p. 1.

¹⁹ Reglamentas (EB) Nr. 765/2008 ir Sprendimas Nr. 768/2008/EB.

²⁰ Ši sistema neapima Sąjungos transporto teisės aktų ir automobilius reglamentuojančių teisės aktų.

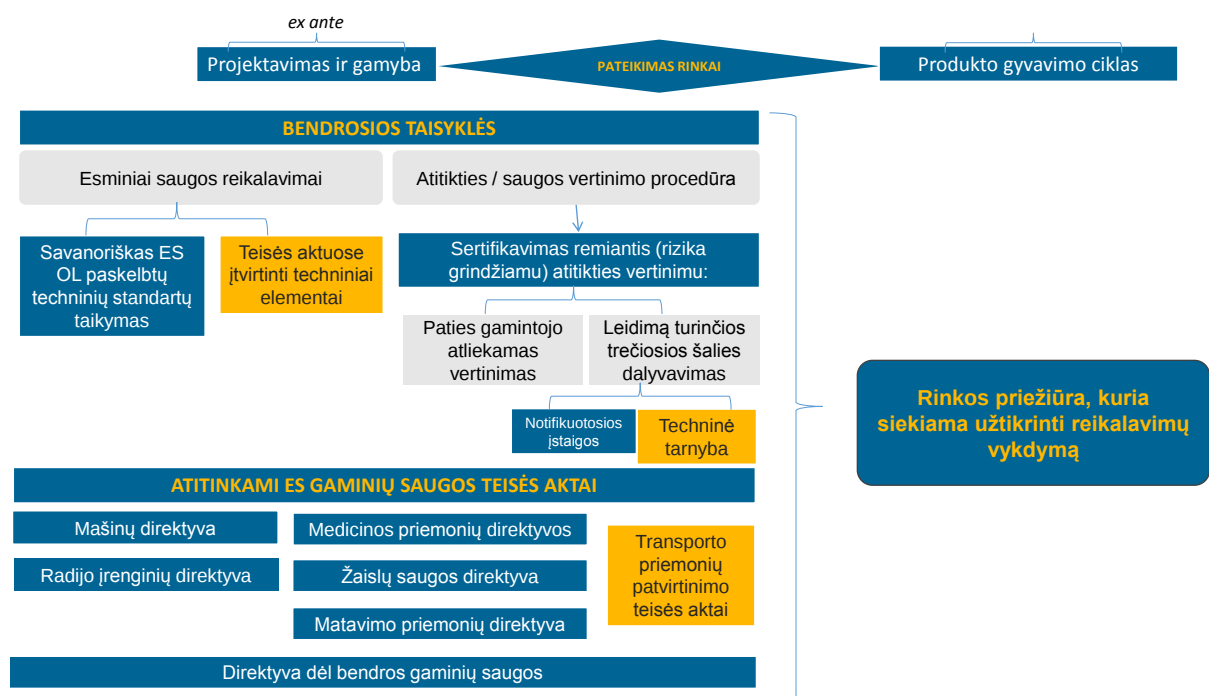
²¹ 2001 m. gruodžio 3 d. Europos Parlamento ir Tarybos direktyva 2001/95/EB dėl bendros gaminių saugos (OL L 11, 2002 1 15, p. 4–17).

²² 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 765/2008, nustatantis su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinant Reglamentą (EEB) Nr. 339/93 (OL L 218, 2008 8 13, p. 30–47, <https://eur-lex.europa.eu/eli/reg/2008/765/oj?locale=lt>), o nuo 2021 m. ir 2019 m. birželio 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/1020 dėl rinkos priežiūros ir gaminių atitikties, kuriuo iš dalies keičiama Direktyva 2004/42/EB ir reglamentai (EB) Nr. 765/2008 ir (ES) Nr. 305/2011 (OL L 169, 2019 6 25, p. 1–44, <https://eur-lex.europa.eu/eli/reg/2019/1020/oj?locale=lt>).

²³ Direktyvos dėl bendros gaminių saugos 8 straipsnio 1 dalies b punkto 3 papunktis.

²⁴ Pavyzdžiui, Direktyva 2007/46/EB dėl motorinių transporto priemonių ir jų priekabų bei tokioms transporto priemonėms skirtų sistemų, sudėtinių dalių ir atskirų techninių mazgų patvirtinimo ir 2018 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/858 dėl motorinių transporto priemonių ir jų priekabų bei tokioms transporto priemonėms skirtų sistemų, komponentų ir atskirų techninių mazgų patvirtinimo ir rinkos priežiūros, kuriuo iš dalies keičiami reglamentai (EB) Nr. 715/2007 ir (EB) Nr. 595/2009 bei panaikinama Direktyva 2007/46/EB.

Dabartinių Sąjungos gaminių saugos teisės aktų loginis pagrindas²⁵



Toliau aptariami uždaviniai, kuriuos besiformuojančios skaitmeninės technologijos kelia Sąjungos gaminių saugos sistemai.

Viena iš pagrindinių vis didesnio skaičiaus produktų ir paslaugų savybių yra **sąsajumas**. Ši savybė gaminio saugai gali pakenkti ir tiesiogiai, ir netiesiogiai (kai į gaminį įsilaužiama ir dėl to kyla grėsmė saugumui bei nukenčia naudotojų sauga), todėl tradicinė saugos samprata jau yra nebepakankama.

Kaip pavyzdį galima paminėti Islandijos per ES skubaus išpėjimo sistemą pateiktą pranešimą dėl vaikiško išmaniojo laikrodžio²⁶. Šis gaminys jį seginčiam vaikui tiesioginės žalos nedaro, tačiau, neužtikrinus būtinojo saugumo lygio, jį galima lengvai naudoti kaip priegios prie vaiko priemonę. Viena iš numatytųjų gaminio paskirčių – užtikrinti vaiko saugumą nustatant jo buvimo vietą, todėl vartotojas tikisi, kad gaminys nekels grėsmės vaiko saugumui, taigi ir jo saugai (t. y. kad vaikas negalės būti sekamas ir (arba) su juo ne bet kas galės susisiekti).

Kitas pavyzdys pateiktas Vokietijos pranešime dėl lengvojo automobilio²⁷. Automobilyje įmontuotoje radijo ryšio įrangoje gali būti tam tikrų programinės įrangos saugumo spragų, kuriomis pasinaudojusios trečiosios šalys gali be leidimo prisijungti prie susietųjų automobilio valdymo sistemų. Jeigu trečioji šalis šiomis programinės įrangos saugumo spragomis pasinaudotų piktavališkais tikslais, galėtų įvykti kelių eismo įvykis.

Neužtikrinus būtinojo pramoninių prietaikų saugumo lygio, joms taip pat galėtų kilti kibernetinių grėsmių, kurių poveikis žmonių saugai būtų didesnis. Tai galėtų būti, pavyzdžiui, kibernetiniai išpuoliai prieš itin svarbią pramonės įmonės valdymo sistemą siekiant sukelti sprogimą, dėl kurio galėtų žūti žmonių.

²⁵ Šiame paveiksle pateikiamas tik bendras pavyzdys – į jį neįtraukti teisės aktuose, kuriais reglamentuojamas produktų gyvavimo ciklas, nustatyti reikalavimai (t. y. naudojimo ir priežiūros reikalavimai).

²⁶ ES interneto svetainėje „Saugūs vartai“ paskelbtas Islandijos RAPEX pranešimas (A12/0157/19).

²⁷ ES interneto svetainėje „Saugūs vartai“ paskelbtas Vokietijos RAPEX pranešimas (A12/1671/15).

Konkrečių privalomų esminių reikalavimų, kuriais siekiama išvengti kibernetinių grėsmių, darančių poveikį naudotojų saugai, Sąjungos gaminių saugos teisės aktuose iš esmės nėra. Tačiau Reglamente dėl medicinos priemonių²⁸, Direktyvoje dėl matavimo priemonių²⁹, Radijo įrenginių direktyvoje³⁰ arba transporto priemonių tipo patvirtinimo teisės aktuose³¹ yra nuostatų, susijusių su saugumo aspektais. Kibernetinio saugumo aktu³² nustatyta savanoriško informacinių ir ryšių technologijų (IRT) produktų, paslaugų ir procesų kibernetinio saugumo sertifikavimo sistema, o atitinkamuose Sąjungos gaminių saugos teisės aktuose nustatyti privalomi reikalavimai.

Be to, sauga taip pat gali nukentėti dėl rizikos, kad besiformuojančios skaitmeninės technologijos gali prarasti tarpusavio ryšį. Pavyzdžiui, susietasis gaisro signalizatorius nutrūkus ryšiui gali neperspėti naudotojo apie kilusį gaisrą.

Dabartiniuose Sąjungos gaminių saugos teisės aktuose sauga yra vienas iš viešosios politikos tikslų. Saugos samprata apima gaminio naudojimą ir pavojus (pvz., susijusius su mechaninėmis savybėmis, elektros naudojimu ir kt.), kuriuos pašalinus gaminys yra saugus. Pažymėtina, kad tam tikruose Sąjungos gaminių saugos teisės aktuose gaminio naudojimo samprata reiškia ne tik numatomą, bet ir numanomą gaminio naudojimą, o kai kuriuose iš jų, pavyzdžiui, Mašinų direktyvoje³³, net ir pagrįstai numanomą netinkamą naudojimą.

Dabartiniuose Sąjungos gaminių saugos teisės aktuose saugos sąvoka yra pakankamai plati, kad būtų galima apsaugoti vartotojus ir naudotojus. Ji apima apsaugą nuo visų rūšių pavojų, kuriuos gali kelti gaminys, įskaitant ne tik su mechaninėmis bei cheminėmis savybėmis ar elektros naudojimu susijusius pavojus, bet ir kibernetinius pavojus bei pavojus, kurie kyla prietaisams praradus tarpusavio ryšį.

Siekiant užtikrinti geresnę naudotojų apsaugą ir suteikti daugiau teisinio tikrumo, būtų galima apsvarstyti galimybę į atitinkamus Sąjungos teisės aktus įtraukti išsamias su minėtais dalykais susijusias nuostatas.

Viena iš pagrindinių dirbtinio intelekto savybių – **autonomiškumas**³⁴. Nenumatytos dirbtinio intelekto naudojimo pasekmės gali būti žalingos naudotojams ir kitiems susijusiems asmenims.

Būsimą dirbtinio intelekto produktų elgseną gamintojas gali nustatyti iš anksto, atlikdamas rizikos vertinimą kol produktai dar nepateikti rinkai, todėl Sąjungos gaminių saugos sistemoje jau nustatytos gamintojų pareigos atliekant rizikos vertinimą atsižvelgti į gaminių

²⁸ Reglamentas (ES) 2017/745 dėl medicinos priemonių.

²⁹ Direktyva 2014/32/ES dėl matavimo priemonių tiekimo rinkai.

³⁰ Radijo įrenginių direktyva (Direktyva 2014/53/ES).

³¹ Direktyva 2007/46/EB dėl motorinių transporto priemonių ir jų priekabų bei tokioms transporto priemonėms skirtų sistemų, sudėtinių dalių ir atskirų techninių mazgų patvirtinimo. Ši direktyva 2020 m. rugsėjo 1 d. bus panaikinta ir pakeista Reglamentu (ES) 2018/858 dėl motorinių transporto priemonių ir jų priekabų bei tokioms transporto priemonėms skirtų sistemų, komponentų ir atskirų techninių mazgų patvirtinimo, kuriuo iš dalies keičiami reglamentai (EB) Nr. 715/2007 ir (EB) Nr. 595/2009 bei panaikinama Direktyva 2007/46/EB.

³² Reglamentas (ES) 2019/881.

³³ Direktyva 2006/42/EB dėl mašinų.

³⁴ Nors dirbtiniu intelektu grindžiami produktai gali būti autonomiški, t. y. įvertinti savo aplinką ir nesilaikyti iš anksto nustatytų komandų, jų elgseną riboja kūrėjų nustatytas tikslas ir kiti atitinkami kūrėjų projektavimo sprendimai.

naudojimą³⁵ per visą jų gyvavimo laikotarpį. Toje sistemoje taip pat numatyta, kad gamintojai naudotojams privalo pateikti instrukcijas ir saugos informaciją arba įspėjimus³⁶. Pavyzdžiui, Radijo įrenginių direktyvoje³⁷ reikalaujama, kad gamintojas pateiktų instrukcijas, kuriose nurodoma, kaip radijo įrenginius naudoti pagal numatytą paskirtį.

Ateityje taip pat gali pasitaikyti atvejų, kai dirbtinio intelekto sistemų naudojimo rezultatai nebus galima visiškai numatyti iš anksto. Todėl rizikos vertinimas, atliktas prieš pateikiant produktą rinkai, gali nebeatspindėti jo naudojimo pobūdžio, veikimo ar elgsenos. Galbūt tokiais atvejais, kai dėl savarankiškai besimokančio produkto autonomiškumo pasikeičia gamintojo iš pradžių numatytas produkto naudojimo pobūdis³⁸ ir tai turi įtakos atitinkamai saugos reikalavimams, reikėtų reikalauti atlikti pakartotinį tokio produkto vertinimą³⁹.

Pagal dabartinę sistemą jau reikalaujama, kad gamintojas, sužinojęs, jog jo gaminys per savo gyvavimo ciklą kelia pavojų saugai, nedelsdamas apie tai informuotų kompetentingas institucijas ir imtųsi veiksmų naudotojams nuo rizikos apsaugoti⁴⁰.

Būtų galima nustatyti naują rizikos vertinimo procedūrą, kuri, be rizikos vertinimo, atliekamo prieš pateikiant gaminį rinkai, būtų taikoma tuo atveju, jei gaminys per savo gyvavimo laikotarpį iš esmės pasikeistų, pavyzdžiui, įgytų kitokią funkciją, kurios gamintojas nenumatė pradiniam rizikos vertinime. Taikant tą procedūrą turėtų būti vertinamas produkto autonomiškumo poveikis saugai per visą jo gyvavimo laikotarpį. Tokį rizikos vertinimą turėtų atlikti atitinkamas ekonominės veiklos vykdytojas. Be to, atitinkamuose Sąjungos teisės aktuose gamintojams galėtų būti nustatyti griežtesni reikalavimai dėl naudotojams skirtų instrukcijų ir įspėjimų.

³⁵ Pagal Sąjungos gaminių saugos teisės aktus atlikdami rizikos vertinimą gamintojai privalo atsižvelgti į numatomą bei numanomą gaminio naudojimą ir (arba) pagrįstai numanomą netinkamą naudojimą.

³⁶ 2008 m. liepos 9 d. Europos Parlamento ir Tarybos sprendimas Nr. 768/2008/EB dėl bendrosios gaminių pardavimo sistemos ir panaikinant Sprendimą 93/465/EEB (OL L 218, 2008 8 13, p. 82–128). I priedo R2 straipsnio 7 dalyje nustatyta: „Gamintojai užtikrina, kad prie gaminio būtų pridėti nurodymai ir saugumo informacija kalba, kuri gali būti lengvai suprantama vartotojams ir kitiems galutiniams naudotojams, kaip nustatė atitinkama valstybė narė.“

³⁷ 10 straipsnio 8 dalis, kurioje minimos galutiniam naudotojui skirtos instrukcijos, ir VI priedas, kuriame nurodyta ES atitikties deklaracija.

³⁸ Kalbant apie dirbtinį intelektą, terminas „savarankiškas mokymasis“ dažniausiai reiškia, kad mašinos yra pajėgios mokytis, kai jos yra mokomos; kol kas nereikalaujama, kad dirbtinio intelekto mašinos mokytųsi ir po to, kai jos pradamos naudoti. Netgi priešingai, visų pirma sveikatos priežiūros srityje dirbtinio intelekto mašinos po sėkmingų mokymų paprastai toliau nebesimoko. Todėl tai, kad produktas dėl dirbtinio intelekto sistemų yra autonomiškas, kol kas nereiškia, kad jis atlieka kūrėjų nenumatytas užduotis.

³⁹ Tai atitinka 2016 m. Mėlynojo vadovo dėl gaminių reglamentuojančių ES taisyklių įgyvendinimo 2.1 skirsnį.

⁴⁰ 2001 m. gruodžio 3 d. Europos Parlamento ir Tarybos direktyvos 2001/95/EB dėl bendros gaminių saugos 5 straipsnis.

Panašius rizikos vertinimus jau reikalaujama atlikti transporto teisės aktuose⁴¹. Pavyzdžiui, geležinkelių transporto teisės aktuose nustatyta, kad tuo atveju, kai modifikuojama jau sertifikuota geležinkelių transporto priemonė, ją modifikuojantis subjektas turi laikytis specialios procedūros ir turi būti taikomi aiškūs kriterijai, pagal kuriuos nustatoma, ar toje procedūroje turi dalyvauti valdžios institucija.

Dirbtinio intelekto produktai ir sistemos mokosi savarankiškai, todėl mašinos gali priimti sprendimus, nukrypstančius nuo to, ką iš pradžių numatė gamintojai, taigi ir nuo to, ko tikisi naudotojai. Tai kelia klausimų dėl žmogaus vykdomos kontrolės: žmonėms turėtų būti suteikta galimybė rinktis, ar leisti dirbtinio intelekto produktams ir sistemoms patiems priimti sprendimus siekiant žmogaus nustatytų tikslų ir kaip tai padaryti⁴². Žmogaus vykdoma savarankiškai besimokančių dirbtinio intelekto produktų ir sistemų priežiūra dabartiniuose Sąjungos gaminių saugos teisės aktuose išsamiai neregamentuojama⁴³.

Atitinkamuose Sąjungos teisės aktuose galėtų būti numatyti konkretūs reikalavimai dėl žmogaus vykdomos priežiūros (kaip apsaugos priemonės), taikomi tiek projektavimo etapu, tiek per visą dirbtinio intelekto produktų ir sistemų gyvavimo ciklą.

Būsimas dirbtinio intelekto prietaikų elgesys taip pat galėtų kelti pavojų naudotojų **psichikos sveikatai**⁴⁴, pavyzdžiui, jei naudotojai namuose ar darbe bendrauja su humanoidiniais dirbtinio intelekto robotais ir sistemomis. Kalbant apie tai, šiandieninė saugos samprata dažniausiai reiškia naudotojo numanomą besiformuojančių skaitmeninių technologijų keliamą fizinės žalos grėsmę. Be to, Sąjungos teisinėje sistemoje saugiais gaminiiais laikomi gaminiai, nekeliantys jokio arba keliantys tik minimalų pavojų žmonių saugai ir sveikatai. Visuotinai pripažįstama, kad sveikatos apibrėžtis apima tiek fizinę, tiek psichinę gerovę. Tačiau psichikos sveikatai keliamas pavojus turėtų būti aiškiai įtrauktas į teisės aktų sistemoje vartojamą gaminių saugos sąvoką.

Pavyzdžiui, technologijų autonomiškumas neturėtų kelti pernelyg didelio ilgalaikio streso bei nepatogumų ir kenkti psichikos sveikatai. Manoma, kad vyresnio amžiaus žmonių saugumo jausmą teigiamai veikia šie veiksniai⁴⁵: saugūs santykiai su sveikatos priežiūros tarnybų darbuotojais, galimybė kontroliuoti kasdienę veiklą ir būti apie tai informuotam. Į šiuos

⁴¹ Jei atliekami geležinkelių sistemos pakeitimai gali turėti įtakos saugai (pvz., jei tai yra techniniai, eksploataciniai arba organizaciniai pakeitimai, galintys turėti įtakos eksploataavimo arba techninės priežiūros procesui), turi būti taikomas Komisijos įgyvendinimo reglamento (ES) 2015/1136 (OL L 185, 2015 7 14, p. 6) I priede aprašytas procesas.

Svarbaus pakeitimo atveju nepriklausoma vertinimo įstaiga (tai galėtų būti nacionalinė saugos institucija arba kita techniniais klausimais kompetentinga institucija) pakeitimą siūlančiam subjektui turėtų pateikti saugos vertinimo ataskaitą.

Pasibaigus rizikos analizės procesui, pakeitimą siūlantis subjektas taikys tinkamas rizikos mažinimo priemones (jei tas subjektas yra geležinkelio įmonė arba infrastruktūros valdytojas, reglamento taikymas yra jo saugos valdymo sistemos, kurios taikymą prižiūri NSI, dalis).

⁴² Aukšto lygio ekspertų grupės dirbtinio intelekto klausimais ataskaita „Politikos ir investicijų rekomendacijos patikimo dirbtinio intelekto srityje“ (*Policy and Investment Recommendations for Trustworthy AI*), 2019 m. birželio mėn.

⁴³ Tačiau tai nereiškia, kad tokia priežiūra nebūtina, – tam tikromis aplinkybėmis šią priežiūrą gali tekti vykdyti dėl kai kurių esamų bendresnių įpareigojimų, susijusių su gaminio pateikimu rinkai.

⁴⁴ PSO įstatų pirmoje įtraukoje teigiama, kad „sveikata yra visiškos fizinės, psichinės ir socialinės gerovės būseną, o ne tik ligos ar negalios nebuvimas“ (<https://www.who.int/about/who-we-are/constitution>).

⁴⁵ *Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction* („Socialiniai robotai. Technologiniai, visuomeniniai ir etiniai žmonių ir robotų sąveikos aspektai“), p. 237–264, *Research, Neziha Akalin, Annica Kristoffersson and Amy Loutfi*, 2019 m. liepos mėn.

veiksnius turėtų atsižvelgti su vyresnio amžiaus žmonėmis bendraujančių robotų gamintojai, kad nekeltų pavojaus tokių žmonių psichikos sveikatai.

Į atitinkamus ES teisės aktus būtų galima įtraukti aiškias gamintojų (įskaitant humanoidinių dirbtinio intelekto robotų gamintojus) pareigas nuodugniai atsižvelgti į nematerialinę žalą, kurią jų gaminiai gali padaryti naudotojams (pirmiausia tiems, kurie yra lengviau pažeidžiami, pavyzdžiui, priežiūros paslaugomis besinaudojantiems pagyvenusiems žmonėms).

Kita svarbi dirbtiniu intelektu grindžiamų produktų ir sistemų savybė – **priklausomybė nuo duomenų**. Siekiant užtikrinti, kad dirbtiniu intelektu grindžiamos sistemos ir produktai sprendimus priimtų taip, kaip numatė gamintojas, labai svarbu, kad jiems teikiami duomenys būtų tikslūs ir aktualūs.

Sąjungos gaminių saugos teisės aktuose klaidingų duomenų keliamas pavojus saugai nėra išsamiai nagrinėjamas. Tačiau, atsižvelgdami į gaminio naudojimo pobūdį, gamintojai dar projektavimo ir bandymo etapais turėtų įvertinti duomenų tikslumo aspektą ir jo svarbą saugos funkcijoms.

Pavyzdžiui, dirbtiniu intelektu grindžiamai sistemai, kurios paskirtis – aptikti konkrečius objektus, gali būti sunku juos atpažinti prastomis apšvietimo sąlygomis, todėl projektuotojai turėtų atsižvelgti į duomenis, gautus atliekant gaminių bandymus tiek įprastomis, tiek prastomis apšvietimo sąlygomis.

Kitas pavyzdys – žemės ūkio (pavyzdžiui, vaisių rinkimo) robotai, kurių funkcija – aptikti prinokusius vaisius ant medžių arba ant žemės. Nors iš naudojamų algoritmų matyti, kad sėkmingai aptinkama daugiau kaip 90 proc. vaisių, jei tiems algoritmams naudojamuose duomenų rinkiniuose būtų trūkumų, tie robotai galėtų priimti netinkamą sprendimą ir sužeisti gyvūną arba žmogų.

Kyla klausimas, ar Sąjungos gaminių saugos teisės aktuose reikėtų nustatyti konkrečius reikalavimus, kuriais klaidingų duomenų keliamas pavojus saugai mažinamas projektavimo etapu, ir mechanizmus, kuriais užtikrinama, kad per visą dirbtinio intelekto produktų ir sistemų naudojimo laiką būtų naudojamosi kokybiškais duomenimis.

Dar viena svarbi kai kurių dirbtiniu intelektu grindžiamų produktų ir sistemų savybė, kurią lemia tų produktų ir sistemų gebėjimas tobulėti mokantis iš patirties, yra **neskaidrumas**. Priklausomai nuo metodologinių sprendimų, dirbtiniu intelektu grindžiamiems produktams ir sistemoms gali būti būdingas įvairaus laipsnio neskaidrumas. Dėl to gali būti sunku atsekti, kaip sistema priima sprendimus (juodosios dėžės reiškinys). Gal žmonėms ir nebūtina perprasti kiekvieno sprendimų priėmimo proceso etapo, tačiau dirbtinio intelekto algoritmai tampa vis pažangesni ir yra diegiami itin svarbiose srityse, todėl labai svarbu, kad žmonės pajėgtų suvokti, kaip sistemos priima algoritminius sprendimus. Tai labai padėtų įgyvendinti *ex post* vykdymo užtikrinimo mechanizmą, nes vykdymo užtikrinimo institucijoms būtų suteikta galimybė atsekti dirbtinio intelekto sistemų elgseną ir pasirinkimus. Tai pripažįstama ir Komisijos komunikate „Pasitikėjimo į žmogų orientuotu dirbtiniu intelektu didinimas“⁴⁶.

Sąjungos gaminių saugos teisės aktuose nėra išsamiai atsižvelgiama į didėjančią riziką, kurią kelia algoritmais grindžiamų sistemų neskaidrumas. Todėl būtina apsvarstyti su algoritmų

⁴⁶ <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>.

skaidrumu, taip pat patikimumu, atskaitomybe ir, kai taikoma, žmogaus vykdoma priežiūra ir nešališkais rezultatais susijusius reikalavimus⁴⁷, kurie yra ypač svarbūs įgyvendinant *ex post* vykdymo užtikrinimo mechanizmą, ir didinti pasitikėjimą minėtomis technologijomis. Vienas iš būdų tai pasiekti – įpareigoti algoritmų kūrėjus nelaimingų atsitikimų atveju atskleisti duomenų rinkinių projektinius parametrus ir metaduomenis.

Pavojų saugai kelia ir **produktų bei sistemų sudėtingumas**, nes įvairūs komponentai, prietaisai ir produktai (pvz., išmaniąją namų ekosistemą sudarantys produktai) gali būti tarpusavyje susieti ir turėti įtakos vienas kito veikimui.

Šis produktų ir sistemų sudėtingumo klausimas jau sprendžiamas šio skirsnio pradžioje minėtoje Sąjungos gaminių saugos teisinėje sistemoje⁴⁸. Joje visų pirma reikalaujama, kad gamintojas, atlikdamas gaminio rizikos vertinimą, atsižvelgtų į numatomą bei numanomą gaminio naudojimą ir, kai taikoma, pagrįstai numanomą netinkamą naudojimą.

Taigi, **jei gamintojas numato, kad jo prietaisas bus susietas ir sąveikaus su kitais prietaisais, į tai jis turėtų atsižvelgti atlikdamas rizikos vertinimą**. Tai, kaip produktas bus naudojamas arba kaip jis gali būti netinkamai naudojamas, nustatoma remiantis, pavyzdžiui, ankstesne tos pačios rūšies produkto naudojimo patirtimi, nelaimingų atsitikimų tyrimais arba žmogaus elgesiu.

Sistemų sudėtingumas taip pat konkrečiau aptariamas atskiriems sektoriams skirtuose gaminių saugos teisės aktuose, pavyzdžiui, Medicinos priemonių reglamente, ir iš dalies bendros gaminių saugos teisės aktuose⁴⁹. Pavyzdžiui, išmaniąjai namų ekosistemai skirtu susietojo prietaiso gamintojas turėtų gebėti pagrįstai numatyti, kad jo produktas darys poveikį kitų produktų saugai.

Transporto teisės aktuose sudėtingumo klausimas sprendžiamas sistemos lygmeniu. Automobilių, traukinių ir lėktuvų tipo patvirtinimo ir sertifikavimo reikalavimai taikomi tiek visai transporto priemonei ar orlaiviui, tiek kiekvienam jų komponentui. Saugos vertinimą sudaro techninė apžiūra ir atitikties tinkamumo skraidyti bei geležinkelių sąveikumo reikalavimams vertinimas. Transporto sektoriuje taikomas sistemos privalo patvirtinti institucija, remdamasi trečiosios šalies atliktu atitikties aiškiems techniniams reikalavimams vertinimu arba paaiškinimu, kaip buvo pašalinta rizika. Sprendimas paprastai būna suderintas produkto ir sistemos lygmenimis.

Sąjungos gaminių saugos teisės aktuose, įskaitant transporto teisės aktus, į gaminių ar sistemų sudėtingumą jau iš dalies atsižvelgiama siekiant sumažinti naudotojų saugai kylantį pavojų.

Sudėtingose sistemose dažnai naudojama **programinė įranga** – ji yra esminis dirbtiniu intelektu grindžiamos sistemos komponentas. Galutinio produkto gamintojas, atlikdamas pradinį rizikos vertinimą, paprastai privalo numatyti į rinkai pateikiamą produktą įdiegtos programinės įrangos keliamą pavojų.

⁴⁷ Remiantis pagrindiniais reikalavimais, kuriuos Aukšto lygio ekspertų grupė pasiūlė „Patikimo dirbtinio intelekto etikos gairėse“ (<https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>).

⁴⁸ Reglamentas (EB) Nr. 765/2008, Sprendimas Nr. 768/2008/EB ir suderinti atskiriems sektoriams skirti gaminių saugos teisės aktai, pvz., Mašinų direktyva (Direktyva 2006/42/EB).

⁴⁹ Direktyvos dėl bendros gaminių saugos 2 straipsnyje nustatyta, kad gaminys yra saugus, jei jį projektuojant atsižvelgiama į „poveikį kitiems gaminiams, kai galima pagrįstai numatyti, kad jis bus naudojamas kartu su kitais gaminiais“.

Tam tikruose Sąjungos gaminių saugos teisės aktuose aiškiai paminėta į gaminį įdiegta programinė įranga. Pavyzdžiui, Mašinų direktyvoje⁵⁰ reikalaujama, kad valdymo sistemos programinės įrangos triktis nesukeltų pavojingų situacijų.

Remiantis Sąjungos gaminių saugos teisės aktais, programinės įrangos atnaujinimą būtų galima palyginti su techninės priežiūros operacijomis, atliekamomis dėl saugos priežasčių, jeigu rinkai jau pateiktas gaminys dėl naujinių iš esmės nepasikeičia ir nekelia naujos rizikos, kuri nebuvo numatyta pradiname rizikos vertinime. Tačiau jei gaminys dėl įdiegto programinės įrangos naujinio iš esmės pasikeičia, jis gali būti laikomas nauju gaminiu ir tuo metu, kai jis pakeičiamas, turi būti iš naujo įvertinta atitiktis atitinkamiems gaminių saugos teisės aktams⁵¹.

Atskiriems sektoriams skirtuose suderintuose Sąjungos gaminių saugos teisės aktuose konkrečių nuostatų dėl autonominės programinės įrangos, kuri atskirai pateikiama rinkai arba diegiama į rinkai jau pateiktą gaminį, iš esmės nėra. Tačiau tokia įranga reglamentuojama tam tikruose Sąjungos teisės aktuose, pavyzdžiui, Medicinos priemonių reglamente. Be to, į tam tikrais radijo moduliais⁵² susietus gaminius įdiegta autonominė programinė įranga taip pat gali būti reglamentuojama pagal Radijo įrenginių direktyvą priimtais deleguotaisiais aktais. Toje direktyvoje reikalaujama, kad tam tikrų klasių ar kategorijų radijo renginiuose būtų funkcijų, kuriomis užtikrinama, kad diegiant programinę įrangą nebūtų pažeista tų įrenginių atitiktis reikalavimams⁵³.

Nors Sąjungos gaminių saugos teisės aktuose atsižvelgiama į pavojų saugai, kurį kelia į rinkai pateikiamą gaminį įdiegta programinė įranga ir galimi gamintojo numatyti tolesni jos naujiniai, gali prireikti nustatyti specialius ir (arba) išsamius reikalavimus dėl autonominės programinės įrangos (pvz., parsisiunčiamų taikomųjų programų). Ypatingas dėmesys turėtų būti skiriamas autonominei programinei įrangai, kuria užtikrinamos dirbtinio intelekto produktų ir sistemų saugos funkcijos.

Siekiant, kad gamintojai įdiegtų funkcijas, kuriomis užtikrinama, kad dirbtinio intelekto produktų gyvavimo laikotarpiu nebūtų įdiegta programinė įranga, dėl kurios nukentėtų sauga, gali prireikti nustatyti papildomas pareigas gamintojams.

Galiausiai, besiformuojančioms skaitmeninėms technologijoms poveikį daro **sudėtingos vertės grandinės**. Tačiau ši problema nėra nauja ir nėra susijusi tik su naujomis besiformuojančiomis skaitmeninėmis technologijomis, tokioms kaip dirbtinis intelektas ar daiktų internetas. Ji būdinga ir tokiems produktams kaip, pavyzdžiui, kompiuteriai, aptarnaujantieji robotai ar transporto sistemos.

Pagal Sąjungos gaminių saugos sistemą atsakomybė už gaminio saugą tenka gaminį rinkai pateikusiam gamintojui, nepriklausomai nuo vertės grandinės sudėtingumo. Gamintojai atsako už galutinio gaminio (įskaitant jo dalis, pvz., kompiuterio programinę įrangą) saugą.

Kai kuriuose Sąjungos gaminių saugos teisės aktuose jau yra nuostatų, kuriomis išsamiai reglamentuojami atvejai, kai su konkrečiu gaminiu, prieš jam patenkant į rinką, susijusią veiklą vykdo keli ekonominės veiklos vykdytojai. Pavyzdžiui, Liftų direktyvoje⁵⁴ reikalaujama, kad liftą projektuojantis ir gaminantis ekonominės veiklos vykdytojas pateiktų

⁵⁰ Mašinų direktyvos I priedo 1.2.1 skirsnis.

⁵¹ [2016 m. Mėlynasis vadovas dėl gaminius reglamentuojančių ES taisyklių įgyvendinimo.](#)

⁵² Radijo modulis – elektroninis prietaisas, siunčiantis ir (arba) priimantis dviejų prietaisų tarpusavyje perduodamus radijo signalus (WIFI, „Bluetooth“).

⁵³ Radijo įrenginių direktyvos 3 straipsnio 3 dalies i punktas.

⁵⁴ Pagal Direktyvos 2014/33/ES 16 straipsnio 2 dalį.

įrengėjui⁵⁵ „visus reikiamus dokumentus ir duomenis, kad pastarasis galėtų užtikrinti teisingą ir saugų lifto įrengimą ir išbandymą“. Mašinų direktyvoje reikalaujama, kad įrangos gamintojai teiktų operatoriui informaciją apie tai, kaip tą įrangą įmontuoti į kitas mašinas⁵⁶.

Sąjungos gaminių saugos teisės aktuose atsižvelgiama į vertės grandinių sudėtingumą ir, laikantis bendros atsakomybės principo, nustatomos įvairių ekonominės veiklos vykdytojų pareigos.

Nors ir patvirtinta, kad gamintojui tenkanti atsakomybė už galutinio produkto saugą dabartinėse sudėtingose vertės grandinėse yra pakankama, išsamios nuostatos, kuriomis aiškiai reikalaujama, kad tiekimo grandinėje dalyvaujantys ekonominės veiklos vykdytojai ir naudotojai tarpusavyje bendradarbiautų, galėtų suteikti teisinį tikrumą galbūt dar sudėtingesnėse vertės grandinėse. Visų pirma todėl, kad visi poveikį gaminio saugai darantys vertės grandinės dalyviai (pvz., programinės įrangos gamintojai) ir naudotojai (keičiantys gaminių) prisiimtų atsakomybę ir suteiktų kitam grandinės dalyviui būtiną informaciją ir priemones.

3. Atsakomybė

Sąjungos nuostatos dėl gaminių saugos ir atsakomybės už juos yra du vienas kitą papildantys mechanizmai, kuriais siekiama to paties politikos tikslo – veikiančios bendros prekių rinkos, kuriai būdingas aukštas saugos lygis, t. y. kurioje iki minimumo sumažinama naudotojų patiriamos žalos rizika ir atlyginama dėl defektinių prekių patirta žala.

Šias Sąjungos taisykles papildo atskiros nacionalinės civilinės atsakomybės sistemos, kuriomis užtikrinama, kad būtų atlyginta dėl įvairių priežasčių (pvz., produktų ir paslaugų) patirta žala ir kuriose nustatyta įvairiems asmenims (pvz., savininkams, veiklos vykdytojams ar paslaugų teikėjams) tenkanti atsakomybė.

Nors Sąjungos saugos taisyklės pritaikius dirbtiniam intelektui būtų galima išvengti nelaimingų atsitikimų, jų tikimybė vis tiek išlieka. Tokiems atvejams numatyta civilinė atsakomybė. Civilinės atsakomybės taisyklės mūsų visuomenėje atlieka dvejopą vaidmenį: viena vertus, jomis užtikrinama, kad nukentėjusiesiems būtų atlyginta kitų asmenų padaryta žala, kita vertus, atsakingai šaliai jos yra ekonominė paskata tokios žalos vengti. Atsakomybės taisyklėmis visuomet turi būti užtikrinama piliečių apsaugos nuo žalos ir galimybių įmonėms diegti inovacijas pusiausvyra.

Sąjungos atsakomybės sistemos iki šiol yra veiksmingos. Jos grindžiamos lygiagrečiu Direktyvos dėl atsakomybės už gaminius (Direktyva 85/374/EEB), kuria suderinta defektinių gaminių gamintojo atsakomybė, ir kitų atskirų nacionalinės atsakomybės sistemų taikymu.

Atsakomybės už gaminius direktyva suteikia tokio lygio apsaugą, kurios nesuteikia vien nacionalinės kalte grindžiamos atsakomybės taisyklės. Toje direktyvoje nustatyta griežta gamintojo atsakomybės už žalą, patirtą dėl jo gaminių defektų, sistema. Fizinę ar materialinę žalą patyrusi nukentėjusioji šalis turi teisę gauti kompensaciją, jeigu įrodo patirtą žalą,

⁵⁵ Liftų direktyvoje (Direktyvoje 2014/33/ES) įrengėjas laikomas lygiaverčiu gamintojui ir privalo prisiimti atsakomybę už lifto projektavimą, gamybą, montavimą ir pateikimą rinkai.

⁵⁶ Mašinų direktyvos I priedo 1.7.4.2 punkte teigiama: „Kiekvienoje instrukcijoje turi būti, jei reikia, bent jau ši informacija: <...> i) surinkimo, montavimo ir sujungimo nurodymai, įskaitant brėžinius, diagramas ir prijungimo būdus, bei nurodyta važiuoklė ar įranga, ant kurios turi būti montuojamos mašinos<...>.“

gaminio defektą (t. y. kad gaminys nebuvo toks saugus, kokio visuomenė turi teisę tikėtis) ir priežastinį defektinio gaminio ir žalos ryšį.

Atskirose nacionalinėse sistemose nustatytos kalte grindžiamos atsakomybės taisyklės, pagal kurias, norėdami sėkmingai išieškoti žalą iš atsakingo asmens, nukentėjusieji turi įrodyti atsakingo asmens kaltę, patirtą žalą ir priežastinį kaltės bei žalos ryšį. Taip pat taikomos atsakomybė be kaltės reglamentuojančios sistemos, kuriose nacionalinis teisės aktų leidėjas atsakomybę už riziką priskiria konkrečiam asmeniui, todėl nukentėjusiajam nebereikia įrodyti kaltės (defekto) arba priežastinio kaltės (defekto) ir žalos ryšio.

Pagal nacionalines atsakomybės sistemas asmenys, patyrę žalą dėl produktų ar paslaugų, gali pateikti kelis lygiagrečius ieškinius dėl žalos atlyginimo, vadovaudamiesi kalte grindžiamos atsakomybės arba atsakomybės be kaltės taisyklėmis. Tokie ieškiniai dažnai pateikiami skirtingiems atsakingiems asmenims ir jiems taikomos skirtingos sąlygos.

Pavyzdžiui, per automobilio avariją nukentėjęs asmuo paprastai pagal nacionalinę civilinę teisę automobilio savininkui (t. y. asmeniui, kuris yra apsidraudęs motorinių transporto priemonių valdytojų civilinės atsakomybės draudimu) teikia ieškinį dėl atsakomybės be kaltės, vairuotojui – ieškinį dėl kalte grindžiamos atsakomybės, o jei automobilis yra su defektu, teikia ieškinį ir automobilio gamintojui pagal Atsakomybės už gaminius direktyvą.

Suderintose motorinių transporto priemonių draudimo taisyklėse reikalaujama, kad naudojama transporto priemonė būtų apdrausta⁵⁷, todėl praktiškai visais atvejais pirmasis asmuo, į kurį kreipiamasi dėl žalos asmeniui arba turtinės žalos atlyginimo, yra draudikas. Vadovaujantis šiomis taisyklėmis, privalomuoju draudimu nukentėjusiajam atlyginama žala ir apsaugomas apdraustasis asmuo, kuris pagal nacionalinės civilinės teisės taisyklės⁵⁸ privalo atlyginti dėl motorinės transporto priemonės sukulto eismo įvykio patirtą finansinę žalą. Direktyvoje dėl atsakomybės už gaminius nustatytas privalomojo draudimo reikalavimas netaikomas gamintojams. Sąjungos teisės aktuose autonominės transporto priemonės draudimo atžvilgiu nėra traktuojamos kitaip nei įprastos transporto priemonės. Autonominės transporto priemonės, kaip ir visos kitos transporto priemonės, turi būti apdraustos transporto priemonių valdytojų civilinės atsakomybės draudimu, nes tai yra lengviausias būdas atlyginti žalą nukentėjusiajai šaliai.

Tinkamas draudimas gali sušvelninti neigiamus eismo įvykių padarinius, nes juo užtikrinama, kad nukentėjusiajam bus atlyginta be jokių nesklandumų. Aiškios atsakomybės taisyklės padeda draudimo bendrovėms įvertinti riziką ir reikalauti, kad žalą atlygintų galutinai už ją atsakinga šalis. Pavyzdžiui, jeigu eismo įvykis įvyko dėl transporto priemonės defekto, tos transporto priemonės draudikas, atlyginęs žalą nukentėjusiajam, gali reikalauti kompensacijos iš gamintojo.

Tačiau dėl naujų skaitmeninių technologijų, tokių kaip dirbtinis intelektas, daiktų internetas ir robotika, savybių keičiasi tam tikri Sąjungos ir nacionalinių atsakomybės sistemų aspektai ir dėl to gali sumažėti tų sistemų veiksmingumas. Dėl kai kurių iš šių savybių gali būti sunku atsekti žmogaus elgesio sukeltą žalą, kurią pagal nacionalines taisykles būtų galima išieškoti iš atsakingo asmens. Tai reiškia, kad pagal nacionalinę deliktų teisę teikiamus ieškinius dėl atsakomybės gali būti sudėtinga arba pernelyg brangu pagrįsti, todėl nukentėjusiesiems gali

⁵⁷ Motorinėms transporto priemonėms taikomos suderintos taisyklės nustatytos Direktyva 2009/103/EB dėl motorinių transporto priemonių valdytojų civilinės atsakomybės draudimo ir privalomojo tokios atsakomybės draudimo patikrinimo.

⁵⁸ Daugumoje valstybių narių atsakomybė be kaltės tenka asmeniui, kurio vardu užregistruota motorinė transporto priemonė.

būti atlyginta nepakankamai. Svarbu, kad nuo nelaimingų atsitikimų, kurie įvyksta dėl produktų ir paslaugų, įskaitant besiformuojančias skaitmenines technologijas (pvz., dirbtinį intelektą), nukentėjusiems asmenims būtų taikoma ne žemesnio lygio apsauga nei nuo kitų panašių produktų ir paslaugų nukentėjusiems asmenims, kuriems žala atlyginama pagal nacionalinę deliktų teisę. Kitaip sumažėtų visuomenės pritarimas šioms besiformuojančioms technologijoms ir pritrūktų ryžto jomis naudotis.

Reikės įvertinti, ar naujų technologijų keliamos problemos galėtų esamose sistemose lemti teisinį netikrumą dėl to, kaip taikyti galiojančius teisės aktus (pvz., kaip kaltės sąvoka būtų taikoma dėl dirbtinio intelekto patirtos žalos atveju). Tai taip pat galėtų atgrasyti nuo investicijų, be to, gamintojai ir kitos tiekimo grandinėje dalyvaujančios įmonės, ypač Europos MVĮ, patirtų daugiau su informacija ir draudimu susijusių išlaidų. Kita vertus, jei valstybės narės galiausiai imtųsi spręsti nacionalinėms atsakomybės sistemoms kylančius uždavinius, tai galėtų lemti tolesnį susiskaidymą, dėl kurio padidėtų inovacinių dirbtinio intelekto sprendimų diegimo sąnaudos ir sumenktų tarpvalstybinė prekyba bendrojoje rinkoje. Svarbu, kad įmonės žinotų savo civilinės atsakomybės riziką visoje vertės grandinėje ir galėtų ją sumažinti ar jos išvengti ir veiksmingai nuo jos apsidrausti.

Šiame skyriuje aiškinama, kokių problemų besiformuojančios technologijos kelia esamoms sistemoms ir kaip jas būtų galima spręsti. Be to, gali prireikti papildomai apsvarstyti kai kurių sektorių, pavyzdžiui, sveikatos priežiūros sektoriaus, ypatumus.

Produktų, paslaugų ir vertės grandinės sudėtingumas. Per pastaruosius dešimtmečius technologijos ir pramonė iš esmės pasikeitė. Pirmiausia produktai ir paslaugos yra vis labiau tarpusavyje susiję, todėl gali būti nebe taip paprasta juos atskirti vienus nuo kitų, kaip buvo anksčiau. Nors sudėtingi produktai ir vertės grandinės nėra naujas Europos pramonės ar jos reguliavimo modelio reiškinys, reglamentuojant atsakomybę už gaminius ypatingas dėmesys turėtų būti skiriamas programinei įrangai ir dirbtiniam intelektui. Daugelio gaminių veikimas grindžiamas programine įranga, o ji gali turėti įtakos tų gaminių saugai. Programinė įranga, būtina tam, kad gaminių būtų galima naudoti kaip numatyta, gali būti ne tik į jį įdiegta, bet ir tiekiamas atskirai. Be programinės įrangos nei kompiuteris, nei išmanusis telefonas nebūtų naudingi. Tai reiškia, kad tokia įranga gali nulemti materialaus gaminio defektus ir fizinę žalą (žr. programinei įrangai skirtą laukelį ataskaitos dalyje, kurioje aptariami saugos aspektai). Dėl šios priežasties produkto gamintojas galiausiai galėtų būti laikomas atsakingu pagal Atsakomybės už gaminius direktyvą.

Tačiau programinė įranga yra įvairių rūšių ir formų, todėl ne visuomet gali būti paprasta nuspręsti, ar programinė įranga laikytina paslauga ar produktu. Taigi, nors programinė įranga, kuria grindžiamas materialaus produkto veikimas, galėtų būti laikoma to produkto dalimi arba komponentu, kai kurių formų autonominę programinę įrangą klasifikuoti gali būti sudėtingiau.

Nors Atsakomybės už gaminius direktyvoje pateikta gaminio apibrėžtis yra plati, būtų galima labiau patikslinti jos taikymo sritį, kad ji geriau atspindėtų besiformuojančių technologijų sudėtingumą, ir taip užtikrinti, kad dėl gaminių, kurių defektus nulėmė programinė įranga ar kitos skaitmeninės jų ypatybės, patirta žala visuomet būtų atlyginta. Tuo remdamiesi ekonominės veiklos vykdytojai, pavyzdžiui, programinės įrangos kūrėjai, galėtų geriau įvertinti, ar jie gali būti laikomi gamintojais pagal Atsakomybės už gaminius direktyvą.

Dirbtinio intelekto prietaikos dažnai diegiamos **sudėtingoje daiktų interneto aplinkoje**, kurioje tarpusavyje sąveikauja daug įvairių susietųjų prietaisų ir paslaugų. Dėl skirtingų šios sudėtingos ekosistemos skaitmeninių komponentų ir dalyvaujančių subjektų įvairovės gali būti sunku nustatyti, kas nulemia galimą žalą ir kuris asmuo yra už ją atsakingas. Dėl šių

technologijų sudėtingumo gali būti labai sudėtinga nukentėjusiems asmenims įvertinti, kas yra atsakingas už žalą, ir laikytis visų nacionalinėje teisėje nustatytų sąlygų, kad būtų galima sėkmingai ją išieškoti. Tokio vertinimo išlaidos gali būti ekonomiškai nepagrįstos, todėl nukentėjusieji gali nedrįsti reikalauti, kad jų patirta žala būtų atlyginta.

Be to, tais atvejais, kai dirbtiniu intelektu grindžiami produktai ir paslaugos sąveikauja su tradicinėmis technologijomis, bus dar sudėtingiau nustatyti, kas atsakingas už žalą. Pavyzdžiui, autonominiai automobiliai kurį laiką važiuos tais pačiais keliais kaip ir įprasti automobiliai. Kai kuriuose paslaugų sektoriuose (pvz., eismo valdymo ir sveikatos priežiūros) panašaus sudėtingumo situacija susiklostys dėl dalyvių sąveikos, nes juose žmonės priims sprendimus naudodamiesi iš dalies automatizuotomis dirbtinio intelekto sistemomis.

Remiantis Atsakomybės ir naujų technologijų ekspertų grupės naujų technologijų klausimais pateikta ataskaita⁵⁹, būtų galima apsvarstyti galimybę pritaikyti nacionalinius įstatymus, kad jais remdamiesi nukentėjusieji galėtų lengviau įrodyti kaltę dėl dirbtinio intelekto patirtos žalos atveju. Pavyzdžiui, pareiga įrodyti kaltę galėtų būti susieta su (atitinkamo veiklos vykdytojo) atitiktimi konkrečioms teisės aktuose nustatytiems kibernetinio saugumo ar kitiems saugos įpareigojimams: jei šių taisyklių nesilaikoma, pareiga įrodyti kaltę ir priežastinį ryšį galėtų būti pakeista.

Komisija įgyvendina atitinkamą ES iniciatyvą, kuria siekia išsiaiškinti, ar ir koku mastu reikėtų sušvelninti tokių sudėtingų situacijų pasekmes, t. y. palengvinti ir (arba) perkelti nacionalinėse civilinės atsakomybės taisyklėse nustatytą pareigą įrodyti žalą, kai ta žala padaroma naudojantis dirbtinio intelekto prietaikomis.

Pagal Sąjungos teisės aktus, pavyzdžiui, Direktyvą dėl atsakomybės už gaminius, privalomų saugos taisyklių neatitinkantis gaminys laikomas defektiniu gaminiu, nepriklausomai nuo gamintojo kaltės. Tačiau gali būti priežasčių apsvarstyti, kaip pagal direktyvą palengvinti nukentėjusiųjų pareigą įrodyti kaltę: toje direktyvoje remiamasi nacionalinėmis taisyklėmis dėl įrodymų ir priežastinio ryšio nustatymo.

Sąsajumas ir atvirumas. Šiuo metu nėra iki galo aišku, kokie lūkesčiai dėl saugos gali būti susiję su žala, patiriama dėl gaminio kibernetinio saugumo pažeidimų, ir ar tokia žala būtų tinkamai atlyginta pagal Direktyvą dėl atsakomybės už gaminius.

Kibernetinio saugumo spragų gali būti ne tik produktą išleidžiant į apyvartą – jų gali atsirasti ir gerokai vėliau.

Jei kalte grindžiamose atsakomybės sistemose nustatomi aiškūs su kibernetiniu saugumu susiję įpareigojimai, veiklos vykdytojai žino, ką jie turi daryti, kad išvengtų su atsakomybe susijusių pasekmių.

Taikant Direktyvą dėl atsakomybės už gaminius, gali vis dažniau kilti klausimas, ar gamintojas, atsižvelgdamas į pagrįstai numanomą gaminio naudojimą, galėjo numatyti tam tikrus jo pasikeitimus. Pavyzdžiui, gali būti dažniau naudojamas nuostata dėl apsaugos nuo vėlesnių defektų, pagal kurią gamintojas nelaikomas atsakingu už defektą, kurio nebuvo gaminio išleidimo į apyvartą metu, arba nuostata dėl apsaugos nuo gaminio pasikeitimo rizikos, jei defekto nebuvo galima numatyti remiantis naujausiomis tuometinėmis žiniomis. Be to, atsakomybė galėtų būti sumažinta tais atvejais, kai nukentėjusioji šalis neįdiegia su

⁵⁹ *Liability for Artificial Intelligence and other emerging technologies' Report* („Ataskaita dėl atsakomybės už dirbtinį intelektą ir kitas besiformuojančias technologijas“, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199).

sauga susijusių naujinių. Tai galėtų būti laikoma paties nukentėjusio asmens aplaidumu ir dėl jo sumažėtų gamintojo atsakomybė. Numanomo pagrįsto naudojimo sąvoka ir su aplaidumu susiję klausimai, pavyzdžiui, saugos naujinio neįdiegimas, gali tapti vis svarbesni, todėl nukentėjusiems asmenims gali būti sunkiau išieškoti dėl gaminio defekto patirtą žalą.

Autonomiškumas ir neskaidrumas. Autonomiškos dirbtinio intelekto prietaikos atlieka užduotis pačios, joms nereikia iš anksto nustatyti kiekvieno etapo ir galima sumažinti žmogaus vykdomą kontrolę ar priežiūrą arba galiausiai visiškai jos atsisakyti. Tačiau savarankiškai besimokančių mašinų algoritmus suprasti gali būti sudėtinga, o gal net neįmanoma (vadinamasis juodosios dėžės reiškinys).

Ne tik dėl pirmiau aptarto sudėtingumo, bet ir dėl kai kurioms dirbtinio intelekto prietaikoms būdingo juodosios dėžės reiškinio gali būti sunku išieškoti autonomiškų dirbtinio intelekto prietaikų nulemtą žalą. Tam, kad būtų galima suprasti dirbtinio intelekto naudojamus algoritmus ir duomenis, reikia analitinių gebėjimų ir techninių žinių, o nukentėjusiems asmenims tai gali pasirodyti pernelyg brangu. Be to, gauti prieigą prie algoritmų ir duomenų gali būti įmanoma tik bendradarbiaujant su galimai atsakinga šalimi. Todėl nukentėjusieji gali būti praktiškai nepajėgūs išieškoti žalą iš atsakingos šalies. Be to, nėra aišku, kaip įrodyti autonomiškai veikiančio dirbtinio intelekto kaltę arba kokia yra dirbtiniu intelektu besinaudojančio asmens kaltė.

Nacionalinės teisės aktuose jau priimta sprendimų, kaip palengvinti panašiose situacijose atsidūrusiems nukentėjusiems tenkančią pareigą įrodyti kaltę.

Pagrindinis principas, kuriuo grindžiama Sąjungos gaminių sauga ir atsakomybė už gaminius, išlieka tas pats – gamintojai privalo užtikrinti, kad visi rinkai tiekiami gaminiai būtų saugūs per visą savo gyvavimo ciklą ir būtų naudojami taip, kaip galima pagrįstai tikėtis. Tai reiškia, kad gamintojas turėtų užtikrinti, jog dirbtiniu intelektu grindžiamas gaminyje atitiktų tam tikrus saugos parametrus. Jei gaminiui būdingos dirbtinio intelekto funkcijos, naudotojas taip pat turi teisę tikėtis, kad tas gaminyje (ar tai būtų automatinė vejamovė, ar robotas chirurgas) yra saugus.

Autonomiškumas gali turėti įtakos produkto saugai, nes dėl jo gali iš esmės pasikeisti produkto savybės, įskaitant saugos funkcijas. Todėl kyla klausimas, kokiomis sąlygomis dėl produkto savarankiško mokymosi išplečiama gamintojo atsakomybė ir kiek jis turėtų numatyti tam tikrus pokyčius.

Siekiant atsižvelgti į tai, kad produktai gali keistis ir būti keičiami, Direktyvoje dėl atsakomybės už gaminius vartojamą išleidimo į apyvartą sąvoką reikėtų persvarstyti, atidžiai atsižvelgiant į atitinkamus Sąjungos saugos sistemos pakeitimus. Tai taip pat padėtų išaiškinti, kam tenka atsakomybė už produkto pakeitimus.

Remiantis Atsakomybės ir naujų technologijų ekspertų grupės naujų technologijų klausimais pateikta ataskaita⁶⁰, kai kuriems dirbtiniu intelektu grindžiamiems prietaisams ir paslaugoms dėl jų autonomiškumo būdingas specifinis su atsakomybe susijusios rizikos profilis, nes šie prietaisai ir paslaugos gali labai pakenkti tokiems svarbiems teisiniams interesams kaip gyvybė, sveikata bei turtas ir kelti pavojų plačiajai visuomenei. Tai visų pirma būtų galima pasakyti apie viešosiose erdvėse judančius dirbtiniu intelektu grindžiamus prietaisus (pvz.,

⁶⁰ *Liability for Artificial Intelligence and other emerging technologies' Report* („Ataskaita dėl atsakomybės už dirbtinį intelektą ir kitas besiformuojančias technologijas“, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199).

visiškai autonomines transporto priemones, bepiločius orlaivius⁶¹ ir siuntinių pristatymo robotus) arba dirbtiniu intelektu grindžiamas paslaugas, kurioms būdinga panaši rizika (pvz., eismo valdymo paslaugas, skirtas transporto priemonėms nukreipti arba kontroliuoti, arba energijos paskirstymo valdymo paslaugas). Problemos, kurias sistemų autonomiškumas ir neskaidrumas kelia nacionalinei deliktų teisei, galėtų būti sprendžiamos laikantis rizika grindžiamo požiūrio. Atsakomybės be kaltės sistemos galėtų užtikrinti, kad per draudžiamąjį įvykį nukentėjusiam asmeniui būtų atlyginama nepriklausomai nuo kaltės. Reikėtų nuodugniai įvertinti pasirinkimo, kam turėtų tekti atsakomybė be kaltės už tokią su dirbtiniu intelektu kūrimu ir diegimu susijusią veiklą, poveikį ir apsvarstyti rizika grindžiamą požiūrį.

Kalbant apie dirbtinio intelekto prietaikų, kurioms būdingas specifinis rizikos profilis, naudojimą, Komisija norėtų išgirsti nuomonę, ar siekiant veiksmingai atlyginti žalą nukentėjusiesiems gali prireikti taikyti atsakomybės be kaltės, kuri pagal nacionalinės teisės aktus taikoma panašios visuomenei kylančios rizikos (pvz., motorinių transporto priemonių, lėktuvų ar branduolinių elektrinių eksploatavimo) atvejais, sistemą ir koku mastu ją gali reikėti taikyti. Komisija taip pat prašo pateikti nuomonę, ar, remiantis Motorinių transporto priemonių draudimo direktyvos pavyzdžiu, atsakomybės be kaltės sistemą reikėtų susieti su galima pareiga sudaryti draudimo sutartį siekiant užtikrinti, kad žala būtų atlyginta nepriklausomai nuo atsakingo asmens mokumo, ir sumažinti dėl žalos patiriamus nuostolius.

Kalbant apie visų kitų prietaikų, kurios sudaro didžiąją dirbtinio intelekto prietaikų dalį, naudojimą, Komisija svarsto, ar reikia pritaikyti pareigą įrodyti priežastinį ryšį ir kaltę. Šiuo atžvilgiu viena iš problemų, į kurią savo ataskaitoje⁶² atkreipė dėmesį Atsakomybės ir naujų technologijų ekspertų grupė naujų technologijų klausimais, yra padėtis, kai galimai atsakinga šalis nepateikia atsakomybei įvertinti tinkamų duomenų arba nenori jais dalytis su nukentėjusiaja šalimi.

4. Išvada

Naujų skaitmeninių technologijų, tokių kaip dirbtinis intelektas, daiktų internetas ir robotika, atsiradimas kelia naujų problemų, susijusių su produktų sauga ir atsakomybe už juos. Šios problemos yra, pavyzdžiui, sąsajumas, autonomiškumas, priklausomybė nuo duomenų, neskaidrumas, produktų ir sistemų sudėtingumas, programinės įrangos atnaujinimas ir sudėtingesnis saugos valdymas bei sudėtingesnės vertės grandinės.

Dabartiniuose gaminių saugos teisės aktuose, visų pirma Direktyvoje dėl bendros gaminių saugos, Mašinų direktyvoje, Radijo įrenginių direktyvoje ir naujoje teisės aktų sistemoje, yra nemažai spragų, kurias reikia pašalinti. Su įvairių šios sistemos teisės aktų pritaikymu susijęs darbas bus atliekamas nuosekliai ir darniai.

Naujos saugos problemos taip pat lemia naujas atsakomybės problemas. Atsakomybės problemos turi būti sprendžiamos taip, kad būtų užtikrinta tokio paties lygio apsauga, kokia taikoma nuo tradicinių technologijų nukentėjusiems asmenims, ir kartu išlaikoma apsaugos ir technologinių inovacijų poreikių pusiausvyra. Tai padės užtikrinti pasitikėjimą šiomis naujomis besiformuojančiomis skaitmeninėmis technologijomis ir investicijų stabilumą.

⁶¹ Plg. bepiločių orlaivių sistemas, nurodytas 2019 m. gegužės 24 d. Komisijos įgyvendinimo reglamente (ES) 2019/947 dėl bepiločių orlaivių naudojimo taisyklių ir procedūrų.

⁶² *Liability for Artificial Intelligence and other emerging technologies' Report* („Ataskaita dėl atsakomybės už dirbtinį intelektą ir kitas besiformuojančias technologijas“, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199).

Nors galiojantys Sąjungos ir nacionalinės teisės aktai, kuriais reglamentuojama atsakomybė, iš esmės padeda spręsti su besiformuojančiomis technologijomis susijusias problemas, dėl dirbtinio intelekto keliamų problemų masto ir bendro poveikio gali būti sudėtingiau atlyginti nukentėjusiesiems žalą pagrįstais atvejais⁶³. Taigi, dėl žalos patirtų nuostolių paskirstymas pagal dabartines taisykles gali būti neteisingas arba neefektyvus. Siekiant išspręsti šias problemas ir galimo esamos sistemos netikrumo klausimą, būtų galima apsvarstyti galimybę įgyvendinant atitinkamas ES iniciatyvas ir laikantis kryptingo rizika grindžiamo požiūrio (t. y. atsižvelgiant į tai, kad skirtingoms dirbtinio intelekto prietaikoms būdinga skirtinga rizika) atlikti tam tikrus Atsakomybės už gaminius direktyvos ir nacionalinės atsakomybės tvarkos pakeitimus.

⁶³ Žr. Aukšto lygio naujų technologijų ekspertų grupės dirbtinio intelekto klausimais ataskaitą (p. 3) ir Politikos rekomendaciją Nr. 27.2.