



Briselē, 19.2.2020.
COM(2020) 64 final

**KOMISIJAS ZIŅOJUMS PARLAMENTAM, PADOMEI UN EIROPAS
EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI,**

**Ziņojums par mākslīgo intelektu, lietu internetu un robotiku drošuma un atbildības
aspektā**

ZIŅOJUMS PAR MĀKSLĪGO INTELEKTU, LIETU INTERNETU UN ROBOTIKU DROŠUMA UN ATBILDĪBAS ASPEKTĀ

1. Ievads

Mākslīgais intelekts (MI, pazīstams arī kā *AI*)¹, lietu internets (*IoT*)² un robotika mūsu sabiedrībai nesīs jaunas iespējas un ieguvumus. Komisija ir atzinusi šo tehnoloģiju nozīmīgumu un potenciālu, kā arī vajadzību šajās jomās veikt apjomīgas investīcijas.³ Tā ir apņēmusies MI, lietu interneta un robotikas jomā Eiropu padarīt par pasaules līderi. Lai šo mērķi sasniegtu, ir vajadzīgs skaidrs un paredzams tiesiskais regulējums, kurš palīdzētu risināt tehnoloģiskos problēmjautājumus.

1.1. Pašreizējais drošuma un atbildības regulējums

Drošuma un atbildības tiesiskā regulējuma vispārējais mērķis ir nodrošināt, ka visi produkti un pakalpojumi, tostarp tie, kuros integrētas jaunās digitālās tehnoloģijas, darbojas droši, uzticami un konsekventi un ka nodarītais kaitējums tiek novērsts efektīvi. Augsts tādu produktu un sistēmu drošuma līmenis, kuros integrētas jaunās digitālās tehnoloģijas, un stabili mehānismi, kas kompensē nodarīto kaitējumu (t. i., atbildības regulējums), palīdz labāk aizsargāt patērētājus. Tie arī sekmē uzticēšanos šīm tehnoloģijām, kas ir priekšnosacījums, lai nozare un lietotāji tās sāktu plaši izmantot. Tas savukārt palielinās mūsu rūpniecības konkurētspēju un sekmēs Savienības mērķu sasniegšanu⁴. Brīdī, kad aktualizējas tādas jaunas tehnoloģijas kā mākslīgais intelekts, lietu internets un robotika, ir svarīgi, lai būtu skaidrs drošuma un atbildības regulējums, kas nodrošinātu patērētāju aizsardzību un sniegtu juridisko noteiktību uzņēmumiem.

Savienībai ir stabils un uzticams drošuma un produktatbildības tiesiskais regulējums un stabils drošības standartu kopums, ko papildina nesaskaņoti nacionālie tiesību akti atbildības jomā. Kopā tie nodrošina mūsu iedzīvotāju labbūtību vienotajā tirgū un sekmē inovāciju un tehnoloģiju plašāku ieviešanu. Tomēr mākslīgais intelekts, lietu internets un robotika maina daudzu produktu un pakalpojumu iezīmes.

2018. gada 25. aprīlī pieņemtajā paziņojumā “Mākslīgais intelekts Eiropai”⁵ tika izziņots, ka Komisija iesniegs ziņojumu, kurā būs novērtēta jauno digitālo tehnoloģiju ietekme uz pašreizējo drošuma un atbildības regulējumu. Šā ziņojuma mērķis ir apzināt un izpētīt, kādas ir uz MI, lietu internetu un robotiku attiecinātā atbildības un drošības regulējuma iespējamās nepilnības, kā arī potenciālās sekas plašākā nozīmē. Šajā ziņojumā, kurš papildina Balto grāmatu par mākslīgo intelektu, izklāstītās orientējošās norādes ir apspriežamas un ir daļa no plašākas konsultēšanās ar ieinteresētajām personām. Drošuma jautājumiem veltītās sadaļas

¹ Augsta līmeņa ekspertu grupas (*AI HLEG*) izstrādātā mākslīgā intelekta definīcija ir pieejama <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>.

² ITU-T Y.2060 sniegtā lietu interneta definīcija ir pieejama <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>.

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

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

⁵ <https://eur-lex.europa.eu/legal-content/lv/TXT/?uri=COM%3A2018%3A237%3AFIN>.
Ar atbildību saistītās problēmas, kuras aktuālas jauno digitālo tehnoloģiju kontekstā, pirmoreiz apskatītas pievienotajā Komisijas dienestu darba dokumentā (2018) 137 (<https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137>).

pamatā ir Mašīnu direktīvas⁶ izvērtējums⁷ un darbs, kas paveikts kopā ar attiecīgajām ekspertu grupām⁸. Atbildības jautājumiem veltītās sadaļas pamatā ir Produktatbildības direktīvas⁹ izvērtējums¹⁰, attiecīgo ekspertu grupu¹¹ devums un apspriedes ar ieinteresētajām personām. Šā ziņojuma mērķis nav sniegt izsmēlošu pārskatu par spēkā esošajiem noteikumiem par drošumu un atbildību, bet gan pievērsties līdz šim apzinātajiem galvenajiem problēmjautājumiem.

1.2. Mākslīgā intelekta, lietu interneta un robotikas tehnoloģiju iezīmes

Mākslīgajam intelektam, lietu internetam un robotikai ir daudzas kopīgas iezīmes. Tie var sevī apvienot **savienojamību**, **autonomiju** un **datatkarību**, lai veiktu uzdevumus nelielā cilvēka kontrolē vai uzraudzībā vai pilnīgi patstāvīgi. Ar MI aprīkotas sistēmas var arī uzlabot pašas savu sniegumu, mācoties no pieredzes. To **sarežģītību** atspoguļo gan daudzskaitlīgie piegādes ķēdē iesaistītie ekonomikas dalībnieki, gan daudzveidīgie komponenti, daļas, programmatūra, sistēmas vai pakalpojumi, kas kopā veido jaunās tehnoloģiskās ekosistēmas. Turklāt pēc laišanas tirgū tie ir **atvērti** atjauninājumiem un uzlabojumiem. Lielais datu apjoms, paļaušanās uz algoritmiem un MI lēmumu pieņemšanas **necaurredzamība** nozīmē, ka ir grūti prognozēt MI iespējota produkta uzvedību un izprast kaitējuma potenciālos cēloņus. Visbeidzot, MI un lietu interneta produktiem piemītošā savienojamība un atvērtība nozīmē, ka tie var būt neaizsargāti pret **kiberdraudiem**.

1.3. Mākslīgā intelekta, lietu interneta un robotikas pavērtās izdevības

Mākslīgais intelekts, lietu internets un robotika var, piemēram, palīdzēt palielināt lietotāju uzticēšanos jaunajām tehnoloģijām un vairo sabiedrības atbalstu tām, uzlabot produktus, procesus un darījumdarbības modeļus, kā arī palīdzēt Eiropas ražotājiem kļūt efektīvākiem.

Papildus produktivitātes un efektivitātes pieaugumam mākslīgais intelekts sola arī dot cilvēkiem iespēju attīstīt intelektu līdz šim nesasniegtā pakāpē, kas paver iespējas jauniem atklājumiem un var palīdzēt atrisināt dažas no pasaules lielākajām problēmām: ārstēt hroniskas slimības, prognozēt slimību uzliesmojumus, samazināt ceļu satiksmes negadījumus bojāgājušo skaitu, cīnīties pret klimata pārmaiņām vai laikus paredzēt kiberdrošības apdraudējumus.

Šīs tehnoloģijas var sniegt daudzus ieguvumus, proti, uzlabot produktu drošumu un mazināt to neaizsargātību pret konkrētiem riskiem. Piemēram, satīkloti un automatizēti

⁶ Direktīva 2006/42/EK.

⁷ SWD(2018) 161 final.

⁸ Patērētāju drošības tīkls, kas izveidots ar Direktīvu 2001/95/EK par produktu vispārēju drošību, un Direktīvas 2006/42/EK par mašīnām un Direktīvas 2014/53/ES par radioiekārtām ekspertu grupas, ko veido dalībvalstu un nozares pārstāvji un citas ieinteresētās personas, piemēram, patērētāju apvienības.

⁹ Direktīva 85/374/EEK.

¹⁰ COM(2018) 246 final.

¹¹ Atbildības un jauno tehnoloģiju ekspertu grupa tika izveidota, lai Komisijai nodrošinātu speciālās zināšanas par Produktatbildības direktīvas un nacionālo civiltiesiskās atbildības noteikumu piemērojamību un lai palīdzētu izstrādāt pamatprincipus iespējamiem ar jaunajām tehnoloģijām saistītiem piemērojamo tiesību aktu pielāgojumiem. To veido divas apakšgrupas, proti, "Produktatbildības apakšgrupa" un "Jauno tehnoloģiju apakšgrupa", sk.

<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1>.

Jauno tehnoloģiju apakšgrupas ziņojumu par mākslīgo intelektu un citām jaunajām tehnoloģijām atbildības aspektā sk. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

transportlīdzekļi varētu uzlabot ceļu satiksmes drošību, jo lielāko daļu ceļu satiksmes negadījumu pašlaik izraisa cilvēka kļūdas¹². Turklāt lietu interneta sistēmas ir izstrādātas tā, lai tās varētu saņemt un apstrādāt lielu datu apjomu no dažādiem avotiem. Šo plašāko informācijas bāzi varētu izmantot produktu pašpielāgošanās un līdz ar to arī drošuma uzlabošanas vajadzībām. Jaunas tehnoloģijas var palīdzēt efektīvāk produktus atsaukt, piemēram, produkti varētu brīdināt lietotājus, ka radusies drošuma problēma¹³. Ja, lietojot satīklotu produktu, rodas drošuma problēmas, ražotāji var tieši sazināties ar lietotājiem, lai tos brīdinātu par riskiem, un, ja iespējams, tieši novērst problēmu, piemēram, piedāvājot drošuma atjauninājumu. Piemēram, 2017. gadā, atsaucot vienu no savām ierīcēm, viedtālrunu ražotājs atjaunināja programmatūru un atsaukto tālrunu akumulatora jaudu samazināja līdz nullei¹⁴, lai lietotāji bīstamās ierīces pārstatu izmantot.

Turklāt jaunās tehnoloģijas var palīdzēt uzlabot produktu izsekojamību. Piemēram, lietu interneta savienojamības elementi var dot iespēju uzņēmumiem un tirgus uzraudzības iestādēm izsekot bīstamus produktus un apzināt riskus piegādes ķēdēs¹⁵.

Līdztekus iespējām, ko mākslīgais intelekts, lietu internets un robotika var sniegt ekonomikai un mūsu sabiedrībai, pastāv arī risks nodarīt kaitējumu likumīgi aizsargātām interesēm (gan materiālām, gan nemateriālām). Jo plašāks ir pielietojums, jo lielāks ir arī šāda kaitējuma rašanās risks. Šajā kontekstā ir svarīgi analizēt, vai un cik lielā mērā pašreizējais drošuma un atbildības jautājumu tiesiskais regulējums joprojām ir piemērots, lai aizsargātu lietotājus.

2. Drošums

Komisijas paziņojumā “Vairojot uzticēšanos antropocentriskam mākslīgajam intelektam” teikts, ka “*MI sistēmās jābūt integrētiem iestrādātās drošības un automātiskās drošības mehānismiem, lai panāktu, ka tās katrā posmā ir pārbaudāmi drošas, ņemot vērā visu iesaistīto personu fizisko un garīgo drošību*”¹⁶.

Šajā sadaļā izklāstītajā Savienības produktu drošuma tiesību aktu novērtējumā ir analizēts, vai pašreizējais Savienības tiesiskais regulējums ietver relevantus elementus, kas nodrošina, ka jaunajās tehnoloģijās, jo īpaši mākslīgā intelekta sistēmās, ir integrēti drošuma un drošības aspekti.

Šajā ziņojumā galvenokārt aplūkota Produktu vispārējā drošuma direktīva¹⁷, kā arī saskaņotie produktu tiesību akti, kuros ievēroti “jaunās pieejas”¹⁸ horizontālie noteikumi un/vai “jaunais

¹² Tiek lēsts, ka aptuveni 90 % no ceļu satiksmes negadījumiem izraisa cilvēka kļūdas. Sk. Komisijas ziņojumu “Dzīvību glābšana: autotransporta drošības uzlabošana ES” (COM(2016) 0787 final).

¹³ Piemēram, automobiļa vadītājs var saņemt brīdinājumu samazināt ātrumu, ja tālāk uz ceļa noticis negadījums.

¹⁴ ESAO (2018), “Measuring and maximising the impact of product recalls globally: OECD workshop report”, *OECD Science, Technology and Industry Policy Papers*, Nr. 56, *OECD Publishing*, Parīze, <https://doi.org/10.1787/ab757416-en>.

¹⁵ ESAO (2018), “Enhancing product recall effectiveness globally: OECD background report”, *OECD Science, Technology and Industry Policy Papers*, Nr. 58, *OECD Publishing*, Parīze, <https://doi.org/10.1787/ef71935c-en>.

¹⁶ Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai “Vairojot uzticēšanos antropocentriskam mākslīgajam intelektam” (8.4.2019., COM(2019)168 final).

¹⁷ Eiropas Parlamenta un Padomes Direktīva 2001/95/EK (2001. gada 3. decembris) par produktu vispārēju drošību (OV L 11, 15.1.2002., 4.–17. lpp.).

¹⁸ OV C 136, 4.6.1985., 1. lpp.

tiesiskais regulējums” (turpmāk “Savienības produktu drošuma tiesību akti vai regulējums”)¹⁹. Horizontālie noteikumi nodrošina saskaņotību starp nozaru noteikumiem par produktu drošumu.

Savienības produktu drošuma tiesību aktu mērķis ir nodrošināt, ka Savienības tirgū laistie produkti atbilst augstām veselības, drošuma un vides aizsardzības prasībām un ka Savienībā ir brīva šādu produktu aprīte. Nozaru tiesību aktus²⁰ papildina Produktu vispārējā drošuma direktīva²¹, kurā noteikts, ka visām patēriņa precēm, pat ja tās nereglementē Savienības nozaru tiesību akti, jābūt drošām. Drošuma noteikumus papildina tirgus uzraudzība un pilnvaras, kas valstu iestādēm piešķirtas ar Tirgus uzraudzības regulu²² un Produktu vispārējā drošuma direktīvu²³. Transporta jomā ir vēl citi Savienības un nacionālie noteikumi par mehānisko transportlīdzekļu²⁴, gaisakuģu vai kuģu nodošanu ekspluatācijā un skaidri noteikumi, kas reglamentē transportlīdzekļa drošumu ekspluatācijas laikā, t. sk. arī operatoru uzdevumus, kā arī iestāžu uzraudzības uzdevumus.

Vēl viens būtisks Savienības produktu drošuma tiesību aktu elements ir Eiropas standartizācijas process. Ņemot vērā digitalizācijas un jauno digitālo tehnoloģiju globālo raksturu, Eiropas rūpniecības konkurētspējai īpaši svarīga ir starptautiskā sadarbība standartizācijas jomā.

Liela daļa Savienības produktu drošuma regulējuma izstrādāta, pirms parādījās tādas digitālās tehnoloģijas kā mākslīgais intelekts, lietu internets vai robotika. Tāpēc tajā ne vienmēr ir iestrādāti noteikumi, kas skaidri risinātu jaunās problēmas un riskus, ko nes šīs jaunās tehnoloģijas. Tomēr, tā kā pašreizējais produktu drošuma regulējums ir tehnoloģiski neitrāls, tas nenozīmē, ka to nevarētu attiecināt uz produktiem, kuros izmantotas šīs tehnoloģijas. Turklāt vēlāk pieņemtajos tiesību aktos, kas ir daļa no minētā regulējuma, piemēram, medicīnisko ierīču vai automobiļu jomā, jau ir skaidri iztirzāti daži jauno digitālo tehnoloģiju aspekti, piemēram, automatizēti lēmumi, programmatūra kā atsevišķs produkts un savienojamība.

¹⁹ Regula (EK) Nr. 765/2008 un Lēmums (EK) Nr. 768/2008/EK.

²⁰ Šī shēma neietver Savienības tiesību aktus par pārvadājumiem un vieglajiem automobiļiem.

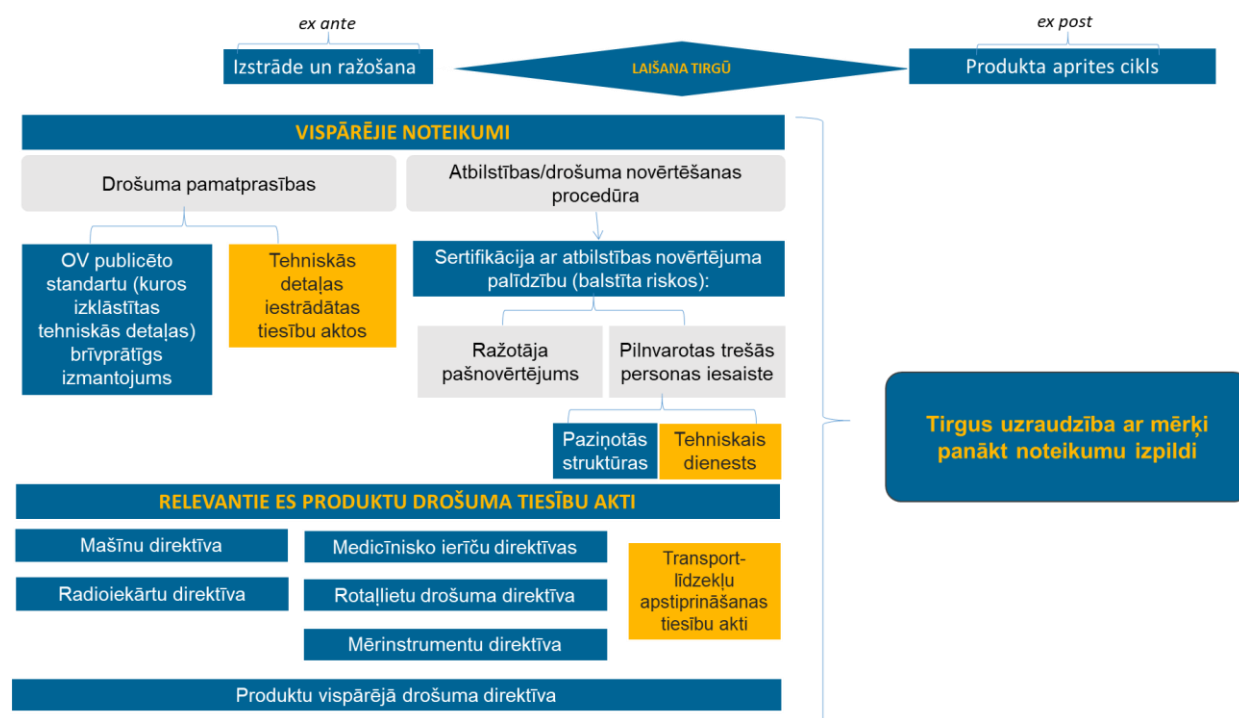
²¹ Eiropas Parlamenta un Padomes Direktīva 2001/95/EK (2001. gada 3. decembris) par produktu vispārēju drošību (OV L 11, 15.1.2002., 4.–17. lpp.).

²² Eiropas Parlamenta un Padomes Regula (EK) Nr. 765/2008 (2008. gada 9. jūlijs), ar ko nosaka akreditācijas un tirgus uzraudzības prasības attiecībā uz produktu tirdzniecību un atceļ Regulu (EEK) Nr. 339/93 (OV L 218, 13.8.2008., 30.–47. lpp., ELI: <http://data.europa.eu/eli/reg/2008/765/oj>) un no 2021. gada Eiropas Parlamenta un Padomes Regula (ES) 2019/1020 (2019. gada 20. jūnijs) par tirgus uzraudzību un produktu atbilstību un ar ko groza Direktīvu 2004/42/EK un Regulas (EK) Nr. 765/2008 un (ES) Nr. 305/201 (OV L 169, 25.6.2019., 1.–44. lpp., ELI: <http://data.europa.eu/eli/reg/2019/1020/oj>).

²³ Produktu vispārējā drošuma direktīvas 8. panta 1. punkta b) apakšpunkta 3) punkts.

²⁴ Piemēram, Direktīva 2007/46/EK, ar ko izveido sistēmu mehānisko transportlīdzekļu un to piekabju, kā arī tādiem transportlīdzekļiem paredzētu sistēmu, sastāvdaļu un atsevišķu tehnisku vienību apstiprināšanai un Eiropas Parlamenta un Padomes Regula (ES) 2018/858 (2018. gada 30. maijs) par mehānisko transportlīdzekļu un to piekabju, kā arī tādiem transportlīdzekļiem paredzētu sistēmu, sastāvdaļu un atsevišķu tehnisku vienību apstiprināšanu un tirgus uzraudzību, ar ko groza Regulas (EK) Nr. 715/2007 un (EK) Nr. 595/2009 un atceļ Direktīvu 2007/46/EK.

Pašreizējo Savienības produktu drošuma tiesību aktu pamatā esošā loģika²⁵



Turpmāk aprakstītas digitālo jauno tehnoloģiju radītās problēmas Savienības produktu drošuma regulējumā.

Aizvien biežāk viena no produktu un pakalpojumu pamatfunkcijām ir **savienojamība**. Šī funkcija apdraud tradicionālo drošuma koncepciju, jo savienojamība produkta drošumu var apdraudēt gan tieši, gan arī netieši, proti, ja produktu var uzlauzt, tas noved pie drošības apdraudējuma un negatīvi ietekmē lietotāju drošumu.

Kā piemēru var minēt ES ātrās brīdināšanas sistēmas paziņojumu no Islandes par bērniem domātu viedpulksteni²⁶. Šis produkts nenodarītu tiešu kaitējumu valkātājam, taču, tā kā tam nebija minimāla drošības līmeņa, to varētu viegli izmantot kā līdzekli, lai piekļūtu bērnam. Tā kā viena no produkta funkcijām ir pasargāt bērnus, izmantojot lokalizāciju, patērētāji sagaida, ka tas neradīs draudus bērna drošībai, nevis dos iespēju kādam bērnu izsekot un/vai ar viņu sazināties.

Vēl viens piemērs atrodams Vācijas iesniegtajā paziņojumā par vieglo automobili²⁷. Transportlīdzeklī uzstādītajam radio var būt daži programmatūras drošības robi, kas nepiederīgām trešām personām atļautu piekļūt transportlīdzekļa savstarpēji satiklotajām vadības sistēmām. Ja trešā persona šos programmatūras drošības trūkumus izmantotu ļaunprātīgos nolūkos, varētu notikt ceļu satiksmes negadījums.

Ja drošības līmenis nav pietiekams, neaizsargāti pret kiberdraudiem var būt arī rūpnieciskie lietojumi, kas ietekmētu cilvēku drošību plašākā mērogā. Te varētu minēt kiberuzbrukumus kritiski svarīgai rūpnīcas vadības sistēmai, piemēram, nolūkā izraisīt sprādzienu, kā rezultātā ietu bojā cilvēki.

²⁵ Attēlā nav iekļautas produktu aprites cikla tiesību aktu prasības, t. i., lietošanas un apkopes prasības, un tas ir sniegts tikai nolūkā sniegt vispārīgu priekšstatu.

²⁶ RAPEX paziņojums no Islandes, kas publicēts ES *Safety Gate* tīmekļvietnē (A12/0157/19).

²⁷ RAPEX paziņojums no Vācijas, kas publicēts ES *Safety Gate* tīmekļvietnē (A12/1671/15).

Savienības produktu drošuma tiesību aktos parasti nav noteiktas specifiskas obligātās pamatprasības attiecībā uz kiberdraudiem, kas ietekmē lietotāju drošību. Tomēr noteikumi par drošības aspektiem ir iestrādāti Medicīnisko ierīču regulā²⁸, Mērinstrumentu direktīvā²⁹, Radioiekārtu direktīvā³⁰ un transportlīdzekļu tipa apstiprinājuma tiesību aktos³¹. Ar Kiberdrošības aktu³² ir izveidots brīvprātīgs kiberdrošības sertifikācijas satvars informācijas un sakaru tehnoloģiju (IST) produktiem, pakalpojumiem un procesiem, savukārt obligātās prasības ir noteiktas relevantajos Savienības produktu drošuma tiesību aktos.

Turklāt risks, ka kādam jauno digitālo tehnoloģiju produktam vai pakalpojumam var zust savienotība, pats par sevi var būt drošuma apdraudējums. Piemēram, ja satīklotam ugunsgrēka signalizatoram zūd savienotība, ugunsgrēka gadījumā tas lietotāju var nebrīdināt.

Pašreizējos Savienības produktu drošuma tiesību aktos drošums ir izvirzīts par publiskā sektora rīcībpolitikas mērķi. Drošuma jēdziens ir saistīts ar produkta lietojumu un riskiem, piemēram, mehāniskiem, elektriskiem u. c., kas jānovērš, lai produkts būtu drošs. Jānorāda, ka dažos Savienības produktu drošuma tiesību aktos produkta lietojums attiecas ne tikai uz paredzēto lietojumu, bet arī uz paredzamo lietojumu un dažos gadījumos, piemēram, Mašīnu direktīvā³³, pat uz pamatoti paredzamu nepareizu lietojumu.

Spēkā esošajos Savienības produktu drošuma tiesību aktos drošuma jēdziens skatīts plašākas drošuma koncepcijas kontekstā, kuras nolūks ir aizsargāt patērētājus un lietotājus. Tādējādi produktu drošuma jēdziens ietver aizsardzību pret visa veida riskiem, ko produkts var izraisīt, tostarp ne tikai mehāniskiem, ķīmiskiem un elektriskiem riskiem, bet arī kiberriskiem un riskiem, kas saistīti ar ierīču savienotības zudumu.

Šajā sakarā, lai nodrošinātu lietotāju labāku aizsardzību un lielāku juridisko noteiktību, vajadzētu apsvērt iespēju relevantajos Savienības tiesību aktos iestrādāt skaidrus noteikumus.

Autonomija³⁴ ir viena no galvenajām mākslīgā intelekta iezīmēm. Ja mākslīgā intelekta darbības gaitā radušies rezultāti ir iepriekš neparedzēti, tas var nodarīt kaitējumu gan lietotājiem, gan pārējām skartajām personām.

Ciktāl mākslīgā intelekta produktu “uzvedību” nākotnē var noteikt jau iepriekš riska novērtējumā, ko ražotājs veic pirms produktu laišanas tirgū, Savienības produktu drošuma regulējumā ražotājiem jau ir noteikts, ka riska novērtējumā jāņem vērā produktu “lietojums”³⁵ visā to kalpošanas laikā. Tajā arī paredzēts, ka ražotājiem jānodrošina

²⁸ Regula (ES) 2017/745 par medicīniskām ierīcēm.

²⁹ Direktīva 2014/32/ES attiecībā uz mērinstrumentu pieejamību tirgū.

³⁰ Direktīva 2014/53/ES par radioiekārtām.

³¹ Direktīva 2007/46/EK – mehānisko transportlīdzekļu un to piekabju, kā arī tādiem transportlīdzekļiem paredzētu sistēmu, sastāvdaļu un atsevišķu tehnisku vienību apstiprināšana. No 2020. gada 1. septembra direktīva tiks atcelta un aizstāta ar Regulu (ES) 2018/858 par mehānisko transportlīdzekļu un to piekabju, kā arī tādiem transportlīdzekļiem paredzētu sistēmu, sastāvdaļu un atsevišķu tehnisku vienību apstiprināšanu un tirgus uzraudzību un ar ko groza Regulas (EK) Nr. 715/2007 un (EK) Nr. 595/2009 un atceļ Direktīvu 2007/46/EK.

³² Regula (ES) 2019/881.

³³ Direktīva 2006/42/EK par mašīnām.

³⁴ Lai gan mākslīgajā intelektā balstīti produkti var darboties autonomi, uztverot apkārtējo vidi un nesejojot iepriekš noteiktām instrukcijām, to uzvedību ierobežo tiem dotais mērķis un citi izstrādātāju noteikti uzbūves parametri. “

³⁵ Savienības produktu drošuma tiesību aktos ir noteikts, ka ražotāji veic riska novērtējumu, balstoties uz produkta paredzēto lietojumu, paredzamo lietojumu un/vai pamatoti paredzamu nepareizu lietojumu.

instrukcijas un drošības informācija lietotājiem vai brīdinājumi³⁶. Tāpēc, piemēram, Radioiekārtu direktīvā³⁷ ir noteikts, ka ražotājam ir jāiekļauj instrukcijas ar informāciju par to, kā radioiekārtas izmantot atbilstoši paredzētajam lietojumam.

Nākotnē varētu rasties arī situācijas, kad mākslīgā intelekta sistēmu radītie iznākumi nav iepriekš pilnībā determinējami. Šādā situācijā riska novērtējums, ko veic pirms produkta laišanas tirgū, varētu arī vairs neatspoguļot produkta lietojumu, funkcionēšanu vai uzvedību. Šādos gadījumos, ja autonomas uzvedības dēļ ražotāja sākotnēji paredzētais lietojums mainās³⁸ un tas ietekmē atbilstību drošības prasībām, varētu prasīt veikt jaunu pašmācīgā produkta atkārtotu novērtējumu³⁹.

Saskaņā ar pašreizējo regulējumu, ja ražotājiem kļūst zināms, ka produkts sava aprites cikla laikā rada risku, kas varētu ietekmēt drošumu, tiem jau tagad ir nekavējoties jāinformē kompetentās iestādes un jāveic pasākumi, lai novērstu risku lietotājiem⁴⁰.

Papildus riska novērtējumam, ko veic pirms produkta laišanas tirgū, varētu ieviest jaunu riska novērtēšanas procedūru gadījumiem, kad ekspluatācijas laikā produkts tiek pakļauts būtiskām izmaiņām, piemēram, produktam ir atšķirīga funkcija, ko ražotājs sākotnējā riska novērtējumā nav paredzējis. Tam būtu jākoncentrējas uz drošuma ietekmējumu, ko rada autonoma uzvedība visā produkta ekspluatācijas laikā. Riska novērtējums būtu jāveic attiecīgajam ekonomikas dalībniekam. Turklāt attiecīgajos Savienības tiesību aktos ražotājiem varētu noteikt stingrākas prasības attiecībā uz lietotājiem domātajām instrukcijām un brīdinājumiem.

Līdzīgi riska novērtējumi jau tiek prasīti transporta tiesību aktos⁴¹; piemēram, dzelzceļa pārvadājumu tiesību akti paredz: ja dzelzceļa transportlīdzeklis pēc tā sertifikācijas tiek pārveidots, pārveidojumu autoram ir piemērojama īpaša procedūra un ir definēti skaidri kritēriji, pēc kuriem nosaka, vai ir jāiesaista attiecīgā iestāde.

³⁶ Eiropas Parlamenta un Padomes Lēmums Nr. 768/2008/EK (2008. gada 9. jūlijs) par produktu tirdzniecības vienotu sistēmu un ar ko atceļ Padomes Lēmumu 93/465/EEK (OV L 218, 13.8.2008., 82.–128. lpp.). I pielikuma R2. panta 7. punktā ir noteikts: “Ražotāji nodrošina, ka produktam ir pievienotas patērētājiem un citiem galalietotājiem viegli saprotamas instrukcijas un drošības informācija valodā, par ko lemj attiecīgā dalībvalsts.”

³⁷ 10. panta 8. punkts, kas attiecas uz galalietotājam domātajām instrukcijām, un VI pielikums, kas attiecas uz ES atbilstības deklarāciju.

³⁸ Līdz šim mākslīgā intelekta kontekstā jēdziens “pašmācīšanās” galvenokārt tiek izmantots, lai norādītu, ka mašīnas apmācības gaitā ir spējīgas mācīties; vēl nav noteikta prasība, ka mākslīgā intelekta iekārtām būtu jāturpina mācīties pēc to ieviešanas; gluži pretēji, jo īpaši veselības aprūpes jomā, pēc tam, kad apmācība ir sekmīgi pabeigta, mākslīgā intelekta iekārtas mācīšanos parasti pārtrauc. Tas nozīmē, ka pašlaik no mākslīgā intelekta sistēmām izrietošā autonomā uzvedība nenozīmē, ka produkts pilda izstrādātāju neparedzētus uzdevumus.

³⁹ Tas atbilst 2.1. iedaļai 2016. gada Zilajā rokasgrāmatā par ES produktu noteikumu īstenošanu.

⁴⁰ Eiropas Parlamenta un Padomes Direktīvas 2001/95/EK (2001. gada 3. decembris) par produktu vispārēju drošību 5. pants.

⁴¹ Komisijas Īstenošanas regulas (ES) 2015/1136 (OV L 185, 14.7.2015., 6. lpp.) I pielikumā ir aprakstīts process, kas jāveic tādu dzelzceļa sistēmas izmaiņu gadījumā, kas var ietekmēt drošumu (piemēram, tehniskas, operacionālas vai arī organizatoriskas izmaiņas, kas varētu ietekmēt ekspluatācijas vai tehniskās apkopes procesu).

Būtisku izmaiņu gadījumā neatkarīgai novērtēšanas iestādei (tā var būt nacionāla drošuma iestāde vai cita tehniski kompetenta iestāde) būtu jāiesniedz izmaiņu ierosinātajam drošuma novērtējuma ziņojums.

Pēc riska analīzes izmaiņu ierosinātais piemēros atbilstošus risku mazināšanas pasākumus (ja ierosinātais ir dzelzceļa pārvadājumu uzņēmums vai infrastruktūras pārvaldītājs, regulas piemērošana ir daļa no tā drošuma pārvaldības sistēmas, kuras piemērošanu uzrauga VDI).

Mākslīgā intelekta produktu un sistēmu pašmācīšanās funkcija var ļaut mašīnai pieņemt lēmumus, kas atšķiras no tā, ko ražotāji bija sākotnēji paredzējuši, un attiecīgi no tā, ko sagaida lietotāji. Tas rada jautājumus par cilvēka kontroli, kur cilvēki varētu izvēlēties, kā un vai deleģēt lēmumu pieņemšanu mākslīgā intelekta produktiem un sistēmām, lai varētu sasniegt cilvēka nospraustos mērķus⁴². Pašreizējos Savienības produktu drošuma tiesību aktos nav eksplicīti aplūkots, kāda loma ir cilvēka pārraudzībai pār mākslīgā intelekta pašmācīšanos produktu un sistēmu kontekstā⁴³.

Attiecīgajos Savienības tiesību aktos varētu paredzēt īpašas prasības par cilvēka realizētu pārraudzību visā MI produktu un sistēmu aprites ciklā, sākot ar produkta izstrādes posmu; šāda pārraudzība varētu kalpot par zināmu aizsarglīdzekli šādos gadījumos.

Mākslīgā intelekta produktu “uzvedība” nākotnē varētu pat **apdraudēt lietotāju garīgo veselību**⁴⁴; tam par cēloni varētu būt, piemēram, sadarbība ar humanoīdiem MI robotiem un sistēmām mājās vai darba vidē. Šajā sakarā mūsdienās uz drošumu parasti atsaucas, runājot par lietotāja priekšstatiem par fiziska kaitējuma draudiem, ko varētu radīt jaunās digitālās tehnoloģijas. Tajā pašā laikā droši produkti Savienības tiesiskajā regulējumā ir definēti kā produkti, kas cilvēku drošībai un veselībai nerada nekādu risku vai rada tikai minimālu risku. Ir vispārpieņemts, ka veselības definīcija ietver gan fizisko, gan garīgo labbūtību. Tomēr tiesiskajā regulējumā produktu drošuma jēdzienam būtu skaidri jāaptver arī garīgās veselības apdraudējums.

Piemēram, autonomijai nevajadzētu radīt pārmērīgu stresu un diskomfortu ilgāku laiku un kaitēt garīgajai veselībai. Šajā sakarā tiek uzskatīts, ka faktori, kas pozitīvi ietekmē vecāka gadagājuma cilvēku drošuma sajūtu⁴⁵, ir šādi: uzturēt stabilas attiecības ar veselības aprūpes dienestu darbiniekiem, spēt kontrolēt ikdienas rutīnu un saņemt informācija par to. Ražotājiem, kuri ražo robotus, kas mijiedarbojas ar vecāka gadagājuma cilvēkiem, šie faktori būtu jāņem vērā, lai novērstu garīgās veselības apdraudējumu.

Varētu apdomāt, vai relevantajos ES tiesību aktos nevajadzētu ražotājiem noteikt skaidru pienākumu (cita starpā attiecībā uz MI humanoīdiem robotiem) noteikti ņemt vērā nemateriālo kaitējumu, ko produkti varētu nodarīt lietotājiem, jo īpaši neaizsargātiem lietotājiem, piemēram, gados veciem cilvēkiem aprūpes iestādēs.

Vēl viena būtiska mākslīgajā intelektā balstītu produktu un sistēmu iezīme ir **datatkarība**. Lai nodrošinātu, ka MI balstītās sistēmas un produkti pieņem lēmumus tā, kā to paredzējis ražotājs, būtiska ir datu precizitāte un relevance.

Savienības produktu drošuma tiesību aktos drošuma apdraudējums, kas izriet no kļūdainiem datiem, nav skaidri aplūkots. Tomēr atkarībā no produkta lietojuma ražotājiem datu precizitāte un relevance drošības funkcijām būtu jāprognozē projektēšanas un testēšanas posmos.

⁴² Mākslīgā intelekta augsta līmeņa ekspertu grupas ieteikumi attiecībā uz rīcībpolitiku un investīcijām uzticamam MI, 2019. gada jūnijs.

⁴³ Tomēr, tā kā pastāv daži vispārīgāki pienākumi attiecībā uz produkta laišanu tirgū, tas neizslēdz, ka konkrētā situācijā uzraudzība var būt nepieciešama.

⁴⁴ PVO konstitūcija, pirmais ievilkums: “Veselība ir pilnīgas fiziskas, garīgas un sociālās labklājības stāvoklis, ne tikai slimību vai traucējumu neesamība.” (<https://www.who.int/about/who-we-are/constitution>)

⁴⁵ Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction, 237.–264. lpp., Research, Nezih Akalin, Annica Kristoffersson un Amy Loutfi, 2019. gada jūlijs.

Piemēram, MI balstītai sistēmai, kas izstrādāta ar mērķi detektēt konkrētus objektus, slikta apgaismojuma apstākļos var būt grūti atpazīt priekšmetus, tāpēc projektētājiem būtu jāiekļauj dati, kas iegūti no produkta testēšanas gan tipiskā, gan slikti apgaismotā vidē.

Vēl viens piemērs ir lauksaimniecības roboti, piemēram, augļu novākšanas roboti, kuru mērķis ir detektēt nogatavojušos augļus uz kokiem vai uz zemes un noteikt to atrašanās vietu. Lai gan iesaistītie algoritmi jau uzrāda sekmīgus klasifikācijas rādītājus (vairāk nekā 90 %), nepilnības datu kopās, kas “baro” šos algoritmus, var novest pie tā, ka šie roboti pieņem sliktu lēmumu un tādējādi ievaino dzīvnieku vai personu.

Rodas jautājums, vai Savienības produktu drošuma tiesību aktos būtu jāiekļauj īpašas prasības, kas būtu vērstas uz drošuma riskiem, kuri saistīti ar kļūdainiem datiem projektēšanas posmā, kā arī mehānismi, kuri nodrošinātu, ka visā MI produktu un sistēmu izmantošanas laikā tiek saglabāta datu kvalitāte.

Necaurredzamība ir vēl viena būtiska dažu MI balstīto produktu un sistēmu iezīme, kas var izrietēt no spējas uzlabot sniegumu, mācoties no pieredzes. Atkarībā no metodiskās pieejas MI balstītus produktus un sistēmas raksturo dažādas necaurredzamības pakāpes. Tas var novest pie grūti izsekojama sistēmas lēmumu pieņemšanas procesa (“melnās kastes efekts”). Cilvēkiem nav obligāti jāsaprot katrs lēmumu pieņemšanas procesa solis, bet, tā kā mākslīgā intelekta algoritmi kļūst sarežģītāki un tiek plašāk izmantoti kritiskās jomās, ir svarīgi, lai cilvēki varētu saprast, kā sistēmas algoritmiskie lēmumi tiek pieņemti. Īpaši svarīgi tas ir izpildes nodrošināšanas *ex post* mehānismam, jo tas tiesībaizsardzības iestādēm dos iespēju izsekot tam, kurš ir atbildīgs par mākslīgā intelekta sistēmu izdarītajām izvēlēm un uzvedību. Tas ir atzīts arī Komisijas paziņojumā “Vairojot uzticēšanos antropocentriskam mākslīgajam intelektam”⁴⁶.

Savienības produktu drošuma tiesību aktos nav skaidri aplūkoti pieaugošie riski, ko rada algoritmos balstītu sistēmu necaurredzamība. Tādēļ ir jāapsver iespēja noteikt prasības par algoritmu caurredzamību, kā arī par robustumu, uzskaitāmību un attiecīgā gadījumā par cilvēka realizētu pārraudzību un objektīviem rezultātiem⁴⁷, kas ir īpaši svarīgi izpildes nodrošināšanas *ex post* mehānismam un lai vairotu uzticību minēto tehnoloģiju izmantošanā. Viens no veidiem, kā risināt šo problēmu, būtu algoritmu izstrādātājiem noteikt pienākumu incidenta gadījumā atklāt datu kopu uzbūves parametrus un metadatus.

Vēl citi riski, kas var ietekmēt drošumu, ir tie, ko rada **produktu un sistēmu sarežģītība**, jo tajās var būt integrēti dažādi komponenti, ierīces un produkti, kuri var ietekmēt cits cita darbību (piem., produkti, kas ir daļa no viedās mājas ekosistēmas).

Šī sarežģītība jau ir apskatīta Savienības drošuma tiesiskajā regulējumā, kas minēts šīs sadaļas sākumā⁴⁸. Proti, ja ražotājs veic produkta riska novērtējumu, tam ir jāņem vērā paredzētais lietojums, paredzamais lietojums un attiecīgā gadījumā pamatoti paredzams nepareizs lietojums.

Šajā kontekstā, **ja ražotājs paredz, ka tā ierīce būs satīklota un mijiedarbosies ar citām ierīcēm, riska novērtējumā tas būtu jāņem vērā.** Lietojumu un nepareizu lietojumu

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

⁴⁷ Pamatojoties uz galvenajām prasībām, ko augsta līmeņa ekspertu grupa ierosinājusi iekļaut Uzticama MI ētiskajās pamatnostādņēs: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>.

⁴⁸ Regula (EK) Nr. 765/2008 un Lēmums (EK) Nr. 768/2008 un saskaņotie nozariskie produktu drošuma tiesību akti, piemēram, Direktīva 2006/42/EK par mašīnām.

nosaka, pamatojoties uz, piemēram, tāda paša veida produkta līdzšinējo lietojumu, incidentu izmeklēšanu vai cilvēku uzvedību.

Sistēmu sarežģītība ir sīkāk apskatīta arī nozariskajos produktu drošuma tiesību aktos, piemēram, Medicīnisko ierīču regulā un zināmā mērā arī Produktu vispārējā drošuma direktīvā⁴⁹. Piemēram, tādas satīklotas ierīces ražotājam, kas iecerēta kā daļa no viedās mājas ekosistēmas, būtu jāspēj saprātīgi paredzēt, ka produkti ietekmēs citu produktu drošumu.

Turklāt transporta tiesību akti šo sarežģītību risina sistēmas līmenī. Viegļajiem automobiļiem, vilcieniem un lidmašīnām tipa apstiprināšana un sertifikācija tiek veikta gan katrai sastāvdaļai, gan visam transportlīdzeklim vai gaisakuģim. Drošuma novērtējumā ietilpst novērtējums par piemērotību dalībai ceļu satiksmē, lidojumderīgumu un dzelzceļa savstarpēju izmantojamību. Transporta nozarē “sistēmas” ir “jāapstiprina” iestādei, vai nu pamatojoties uz trešās personas veiktu novērtējumu par atbilstību skaidrām tehniskajām prasībām, vai arī pēc demonstrējuma, kurā pierāda, kā tiek novērsti riski. Risinājums parasti ir “produkta” un “sistēmas” līmeņa kombinācija.

Savienības produktu drošuma tiesību aktos, tostarp transporta tiesību aktos, produktu vai sistēmu sarežģītība jau zināmā mērā ir ņemta vērā, lai novērstu riskus, kas varētu ietekmēt lietotāju drošību.

Sarežģītas sistēmas bieži vien ietver **programmatūru**, kas ir būtiska MI balstītas sistēmas sastāvdaļa. Parasti sākotnējā riska novērtējuma ietvaros galaprodukta ražotājam ir pienākums paredzēt riskus, kas piemīt produktā integrētajai programmatūrai brīdī, kad produktu laiž tirgū.

Dažos Savienības produktu drošuma tiesību aktos ir skaidra atsauce uz produktā integrēto programmatūru. Piemēram, Mašīnu direktīvā⁵⁰ ir noteikts, ka vadības sistēmas programmatūras kļūme nedrīkst radīt bīstamas situācijas.

Savienības produktu drošuma tiesību aktos programmatūras atjauninājumus varētu pielīdzināt tehniskās apkopes darbībām, ko veic drošuma apsvērumu dēļ, ar nosacījumu, ka tie būtiski nemodificē tirgū jau laistu produktu un nerada jaunus riskus, kas nav paredzēti sākotnējā riska novērtējumā. Tomēr, ja programmatūras atjauninājums būtiski maina produktu, kurā tas lejupielādēts, visu produktu varētu uzskatīt par jaunu produktu un pārveidošanas laikā būtu atkārtoti jāizvērtē atbilstība attiecīgajiem produktu drošuma tiesību aktiem⁵¹.

Attiecībā uz savrupu programmatūru, kas tirgū laista atsevišķi vai augšupielādēta pēc produkta laišanas tirgū, Savienības saskaņotajos nozariskajos produktu drošuma tiesību aktos lielākoties nav īpašu noteikumu. Tomēr dažos Savienības tiesību aktos savrupa programmatūra ir regulēta, piemēram, Medicīnisko ierīču regulā. Turklāt savrupu programmatūru, kas augšupielādēta satīklotos produktos, kuri sazinās, izmantojot konkrētus radio moduļus⁵², var reglamentēt arī Radioiekārtu direktīva, tam izmantojot deleģētos aktus. Šajā direktīvā noteikts, ka dažām radioiekārtu klasēm vai kategorijām ir jābūt funkcijām, kas nodrošina, ka, augšupielādējot programmatūru, netiek apdraudēta šo iekārtu atbilstība⁵³.

⁴⁹ Produktu vispārējā drošuma direktīvas 2. pantā noteikts, ka, lai produkts būtu drošs, ņem vērā “ietekmi uz citiem produktiem, ja paredzams, ka to izmantos kopā ar citiem produktiem”.

⁵⁰ Mašīnu direktīvas I pielikuma 1.2.1. iedaļa.

⁵¹ [“Zilā rokasgrāmata” par ES produktu noteikumu īstenošanu, 2016.](#)

⁵² Radio moduļi ir elektroniska ierīce, kas pārraida un/vai uztver radio signālus (*WIFI, Bluetooth*) starp divām ierīcēm.

⁵³ Radioiekārtu direktīvas 3. panta 3. punkta i) apakšpunkts.

Lai gan Savienības produktu drošuma tiesību aktos ir ņemti vērā no produktā integrētas programmatūras izrietošie drošuma riski laikā, kad to laiž tirgū, un iespējamie vēlākie atjauninājumi, ko paredzējis ražotājs, varētu būt vajadzīgas īpašas un/vai skaidras prasības attiecībā uz savrupu programmatūru (piemēram, “lietotne”, kas tiktu lejupielādēta). Īpaša uzmanība būtu jāpievērš tādai savrupai programmatūrai, kas nodrošina mākslīgā intelekta produktu un sistēmu drošuma funkcijas.

Iespējams, ražotājiem vajadzētu uzlikt papildu pienākumus, kas nodrošinātu, ka tie ir parūpējušies par funkcijām, kas novērš augšupielādētās programmatūras ietekmi uz drošumu MI produkta ekspluatācijas laikā.

Visbeidzot, jaunās digitālās tehnoloģijas ietekmē **sarežģītas vērtību ķēdes**. Tomēr šī sarežģītība ir problēma, kas nav ne jauna, ne tāda, kas būtu parādījusies tikai līdz ar jaunajām digitālajām tehnoloģijām, piemēram, mākslīgo intelektu vai lietu internetu. Te var minēt tādus produktus kā datori, pakalpojumu roboti un transporta sistēmas.

Saskaņā ar Savienības produktu drošuma regulējumu neatkarīgi no tā, cik sarežģīta ir vērtību ķēde, par produkta drošumu joprojām atbild ražotājs, kas produktu laiž tirgū. Ražotāji ir atbildīgi par galaprodukta, tostarp produktā integrēto daļu, piemēram, datora programmatūras, drošumu.

Dažos Savienības produktu drošuma tiesību aktos jau ir noteikumi, kas skaidri reglamentē situācijas, kurās pie kāda konkrēta produkta pirms tā laišanas tirgū strādā vairāki ekonomikas dalībnieki. Piemēram, Liftu direktīvā⁵⁴ noteikts, ka uzņēmējs, kas projektējis un ražojis liftu, uzstādītājam⁵⁵ nodrošina “*visus vajadzīgos dokumentus un informāciju, lai šī persona spētu nodrošināt pareizu un drošu lifta uzstādīšanu un testēšanu*”. Mašīnu direktīvā noteikts, ka iekārtu ražotājiem jāsniedz operatoram informācija par to, kā iekārtu montēt kopā ar citu mašīnu⁵⁶.

Savienības produktu drošuma tiesību aktos vērtību ķēžu sarežģītība ir ņemta vērā, pienākumus vairākiem ekonomikas dalībniekiem nosakot pēc dalītas atbildības principa.

Lai gan ir pierādījies, ka ražotāja atbildība par galaprodukta drošumu ir pietiekama pašreizējā vērtību ķēžu sarežģītības pakāpē, gadījumos, kad vērtību ķēžu sarežģītība vēl vairāk pieaugusi, nepieciešamo juridisko noteiktību varētu nodrošināt skaidri noteikumi, kuros īpaši prasīta sadarbība starp ekonomikas dalībniekiem piegādes ķēdē un lietotājiem. Tas nozīmētu, ka katrs vērtību ķēdes dalībnieks, kas ietekmē produkta drošumu (piemēram, programmatūras ražotāji), un lietotāji (ja tie izmaina produktu) uzņemtos atbildību un nodrošinātu vajadzīgo informāciju un pasākumus nākamajam ķēdes dalībniekam.

3. Atbildība

Savienības līmenī produktu drošuma un produktatbildības noteikumi ir divi savstarpēji papildinoši mehānismi, kas palīdz sasniegt vienu un to pašu rīcībpolitisko mērķi, proti,

⁵⁴ Saskaņā ar Direktīvas 2014/33/ES 16. panta 2. punktu.

⁵⁵ Direktīvā 2014/33/ES jeb Liftu direktīvā ražotāja ekvivalents ir uzstādītājs, un tam jāuzņemas atbildība par lifta projektēšanu, ražošanu, uzstādīšanu un laišanu tirgū.

⁵⁶ Mašīnu direktīvas I pielikuma 1.7.4.2. punktā teikts: “*Katrā instrukciju rokasgrāmatā jābūt pēc iespējas vismaz šādai informācijai: (..) i) montāžas, uzstādīšanas un pieslēgšanas instrukcijas, tostarp rasējumi, diagrammas un stiprinājuma līdzekļi, kā arī šasijas vai konstrukcijas apzīmējums, uz kādas mašīna jāuzmontē;*”.

panākt funkcionējošu vienoto preču tirgu, kas nodrošina augstu drošuma līmeni; tas nozīmē, ka līdz minimumam ir samazināts kaitējuma risks lietotājiem un ir paredzēta kompensācija par kaitējumu, ko rada defektīvas preces.

Valstu līmenī šos Savienības noteikumus papildina nesaskaņoti civiltiesiskās atbildības regulējumi, kuri nodrošina kompensāciju par kaitējumu, kam ir dažādi iemesli (piemēram, produkti vai pakalpojumi), un kuri vērsti uz dažādām atbildīgajām personām (piemēram, īpašnieki, operatori vai pakalpojumu sniedzēji).

Lai gan Savienības MI drošuma noteikumu optimizācija var palīdzēt izvairīties no negadījumiem, tie tomēr nav izslēgti. Tas ir brīdis, kad nāk talkā civiltiesiskā atbildība. Civiltiesiskās atbildības noteikumiem mūsu sabiedrībā ir divējāda funkcija: no vienas puses, tie nodrošina, ka no citu nodarītā kaitējuma cietušie saņem kompensāciju, bet, no otras puses, tie atbildīgajai pusei dod ekonomisku stimulu no šāda kaitējuma radīšanas izvairīties. Noteikumos par atbildību vienmēr ir jārod līdzsvars starp iedzīvotāju aizsardzību pret kaitējumu un uzņēmumu iespējām ieviest jauninājumus.

Atbildības regulējums Savienībā ir darbojies labi. Paralēli tiek piemērota Produktatbildības direktīva (Direktīva 85/374/EEK, ar ko tika saskaņota produktu ražotāja atbildība par defektīviem produktiem) un citi nesaskaņoti nacionālie atbildības regulējumi.

Produktatbildības direktīva nodrošina tādu aizsardzības līmeni, kādu nevar sniegt viens pats nacionālais regulējums par atbildību, kuras priekšnosacījums ir vaina. Ar to tiek ieviesta sistēma, kas paredz ražotāja atbildību par kaitējumu, ko nodarījis tā ražoto produktu defekts, neatkarīgi no ražotāja vainas. Fiziska vai materiāla kaitējuma gadījumā cietušajai personai ir tiesības uz kompensāciju, ja tā pierāda kaitējumu, produkta defektu (t. i., ka tas nav nodrošinājis tādu drošuma līmeni, kādu sabiedrībai ir tiesības sagaidīt) un cēloņsakarību starp defektīvo produktu un kaitējumu.

Nesaskaņotie nacionālie režīmi paredz noteikumus par atbildību, kas balstās uz vainu; saskaņā ar šiem noteikumiem, lai prasība par saukšanu pie atbildības būtu sekmīga, no kaitējuma cietušajiem ir jāpierāda atbildīgās personas vaina, kaitējums un cēloņsakarība starp vainu un kaitējumu. Tajos ir paredzēti arī režīmi par atbildību neatkarīgi no vainas, kur valsts likumdevējs atbildību par risku ir uzlicis konkrētai personai un cietušajam nav jāpierāda vaina/defekts vai cēloņsakarība starp vainu/defektu un kaitējumu.

Nacionālie atbildības režīmi personām, kas cietušas no produktu un pakalpojumu radīta kaitējuma, paredz vairākas paralēlas kompensācijas prasījuma iespējas, kas balstītas uz vainu vai atbildību neatkarīgi no vainas. Šie prasījumi bieži ir vērsti pret dažādām atbildīgajām personām, un tiem ir atšķirīgi nosacījumi.

Piemēram, cietušais, kas iesaistīts ceļu satiksmes negadījumā, parasti prasību par atbildību neatkarīgi no vainas vērš pret automobiļa īpašnieku (t. i., personu, kas iegādājas transportlīdzekļa īpašnieka civiltiesiskās atbildības apdrošināšanu), bet prasību par atbildību, kas balstās uz vainu, – pret automobiļa vadītāju (valsts civiltiesību darbības joma); un, ja automobilim bijis defekts, iesniedz prasību saskaņā ar Produktatbildības direktīvu pret ražotāju.

Saskaņā ar saskaņotajiem noteikumiem par mehānisko transportlīdzekļu apdrošināšanu transportlīdzekļa izmantošanai jābūt apdrošinātai⁵⁷, un praksē apdrošinātājs vienmēr ir pirmā

⁵⁷ Šī norma mehāniskajiem transportlīdzekļiem ir saskaņota ar Direktīvu 2009/103/EK par civiltiesiskās atbildības apdrošināšanu saistībā ar mehānisko transportlīdzekļu izmantošanu un kontroli saistībā ar pienākumu apdrošināt šādu atbildību.

persona, pret ko vērš prasījumu atlīdzināt miesas bojājumus vai mantisko kaitējumu. Saskaņā ar šiem noteikumiem obligātā apdrošināšana sniedz kompensāciju cietušajam un aizsargā apdrošināto personu, kas saskaņā ar valsts civiltiesību normām⁵⁸ ir atbildīga par finansiālu zaudējumu atlīdzināšanu par negadījumu, kurā iesaistīts mehāniskais transportlīdzeklis. Saskaņā ar Produktatbildības direktīvu uz produktu ražotājiem obligātā apdrošināšana neattiecas. Attiecībā uz mehānisko transportlīdzekļu apdrošināšanu autonomie transportlīdzekļi Savienības tiesību aktos ir regulēti tāpat kā neautonomie transportlīdzekļi. Šādiem transportlīdzekļiem, tāpat kā visiem transportlīdzekļiem, ir jābūt apdrošinātiem ar transportlīdzekļa īpašnieka civiltiesiskās atbildības apdrošināšanu, kas ir visvieglākais veids, kā cietušā persona var saņemt kompensāciju.

Pienācīga apdrošināšana var mazināt negadījumu negatīvās sekas, jo tā cietušajam vienkāršo kompensācijas saņemšanu. Skaidri noteikumi par atbildību palīdz apdrošināšanas sabiedrībām aprēķināt savus riskus un pieprasīt atlīdzību no personas, kas patiesībā atbildīga par kaitējumu. Piemēram, ja nelaimes gadījumu ir izraisījis defekts, mehānisko transportlīdzekļu apdrošinātājs pēc kompensācijas izmaksas cietušajam var pieprasīt kompensācijas atmaksu no automobiļa ražotāja.

Tomēr tādu jauno digitālo tehnoloģiju kā mākslīgais intelekts, lietu internets un robotika īpatnības dažos Savienības un nacionālo atbildības sistēmu aspektos rada problēmas un varētu mazināt to iedarbīgumu. Dažas no šīm īpatnībām varētu apgrūtināt izsekot kaitējumu rašanos līdz cilvēka rīcībai, kas varētu dot pamatu uz vainu balstītai prasībai saskaņā ar nacionālajiem noteikumiem. Tas nozīmē, ka var būt grūti vai dārgi pierādīt, ka prasība par atbildību, kura pamatojas uz nacionālajām deliktu tiesībām, ir pamatota, un līdz ar to cietušie var nesaņemt pienācīgu kompensāciju. Ir svarīgi, lai aizsardzības līmenis, kas pienākas personām, kas cietušas negadījumos, kuros iesaistītas preces vai pakalpojumi, kuros izmantotas jaunās digitālās tehnoloģijas, piemēram, mākslīgais intelekts, nebūtu zemāks kā līdzīgu citu produktu un pakalpojumu gadījumā, kur tās būtu tiesīgas saņemt kompensāciju saskaņā ar nacionālajām deliktu tiesībām. Šāda situācija varētu mazināt sabiedrības atbalstu šīm jaunajām tehnoloģijām un novest pie vilcināšanās tās izmantot.

Būs jāizvērtē, vai jauno tehnoloģiju radītie sarežģītumi esošajās sistēmās varētu radīt arī juridisku nenoteiktību tajā, kā būtu piemērojami spēkā esošie tiesību akti (piemēram, kā vainas jēdzienu piemērot mākslīgā intelekta radītam kaitējumam). Tas savukārt varētu atturēt investorus, kā arī ražotājiem un citiem uzņēmumiem piegādes ķēdē, jo īpaši Eiropas MVU, palielināt informēšanas un apdrošināšanas izmaksas. Turklāt, ja dalībvalstis laika gaitā atrisinātu sarežģījumus, ko jaunās tehnoloģijas rada nacionālajās atbildības sistēmās, tas varētu radīt vēl lielāku sadrumstalotību, tādējādi palielinot izmaksas, kas saistītas ar inovatīvu MI risinājumu ieviešanu, un samazinot pārrobežu tirdzniecības apjomus vienotajā tirgū. Ir svarīgi, ka uzņēmumi visā vērtības ķēdē apzinās savus atbildības riskus un var tos samazināt vai novērst un pret tiem efektīvi apdrošināties.

Šajā nodaļā ir paskaidrots, kā jaunās tehnoloģijas rada sarežģījumus esošajās sistēmās un kā šīs problēmas varētu risināt. Turklāt īpatnības, kas raksturīgas dažām nozarēm, piemēram, veselības aprūpei, iespējams, jāapskata padziļināti.

Produktu, pakalpojumu un vērtību ķēdes sarežģītība. Pēdējo desmitgažu laikā tehnoloģijas un rūpniecība ir krasi attīstījušās. Šķērsums starp produktiem un pakalpojumiem ne vienmēr ir tik skaidrs, kā agrāk. Savstarpējās saiknes starp produktiem un pakalpojumu

⁵⁸ Lielākajā daļā dalībvalstu atbildību neatkarīgi no vainas piemēro personai, uz kuras vārda mehāniskais transportlīdzeklis ir reģistrēts.

sniegšanu kļūst arvien ciešākas. Lai gan sarežģīti produkti un vērtību ķēdes Eiropas rūpniecībā un tās regulatīvajā modelī nav jaunums, programmatūra un arī mākslīgais intelekts ir pelnījuši īpašu uzmanību produktatbildības aspektā. Programmatūrai ir būtiska nozīme daudzu produktu darbībā, un tā var ietekmēt to drošumu. Tā ir integrēta produktos, bet to var piegādāt arī atsevišķi, lai produktu varētu izmantot paredzētajam mērķim. Bez programmatūras ne dators, ne viedtālrunis nebūtu īsti izmantojami. Tas nozīmē, ka programmatūra var taustāmu produktu padarīt defektīvu, un tas var radīt fizisku kaitējumu (sk. programmatūrai veltīto ierāmējumu drošuma sadaļā). Tā rezultātā ražotājs var tikt saukts pie atbildības saskaņā ar Produktatbildības direktīvu.

Tomēr, tā kā programmatūra ir sastopama dažādos veidos un formās, ne vienmēr ir viegli saprast, vai programmatūra būtu klasificējama kā pakalpojums vai produkts. Tādējādi, lai gan programmatūru, kas vada taustāma produkta darbību, varētu uzskatīt par šā produkta daļu vai komponentu, cita veida savrupā programmatūra varētu būt grūtāk klasificējama.

Lai gan Produktatbildības direktīvā sniegtā produkta definīcija ir plaša, tās darbības jomu varētu precizēt, lai labāk atspoguļotu jauno tehnoloģiju sarežģītību un nodrošinātu, ka par kaitējumu, ko izraisījuši produkti, kuri kļuvuši defektīvi programmatūras vai citu digitālo funkciju dēļ, vienmēr ir pieejama kompensācija. Tas labāk ļautu ekonomikas dalībniekiem, piemēram, programmatūras izstrādātājiem, novērtēt, vai tos var uzskatīt par ražotājiem saskaņā ar Produktatbildības direktīvu.

Mākslīgā intelekta lietojumi bieži vien ir integrēti **sarežģītās lietu interneta vidēs**, kurās mijiedarbojas daudzas dažādas satīklotas ierīces un pakalpojumi. Dažādas digitālo komponentu apvienojums sarežģītā ekosistēmā un iesaistīto dalībnieku daudzskaitlīgums var novest pie tā, ka ir grūti novērtēt, kur sakņojas iespējamais kaitējums un kura persona par to ir atbildīga. Šo tehnoloģiju sarežģītības dēļ cietušajiem var būt ļoti grūti identificēt atbildīgo personu un izpildīt visus valsts tiesību aktos noteiktos nosacījumus, lai prasība būtu sekmīga. Šādas ekspertīzes izmaksas var būt ļoti augstas un atturēt cietušos no kompensācijas pieprasīšanas.

Turklāt produkti un pakalpojumi, kuri balstīti uz mākslīgo intelektu, mijiedarbojas ar tradicionālajām tehnoloģijām, tādējādi vēl vairāk apgrūtinot atbildības noteikšanu. Piemēram, autonomie automobiļi zināmu laiku dalīs ceļu ar tradicionālajiem automobiļiem. Līdzīga sarežģītība, ko rada mijiedarbība starp aktoriem, rodas arī dažās pakalpojumu nozarēs (piemēram, satiksmes pārvaldībā un veselības aprūpē), kurās cilvēkiem pieņemt lēmumus palīdzēs daļēji automatizētas mākslīgā intelekta sistēmas.

Saskaņā ar Atbildības un jauno tehnoloģiju ekspertu grupas Jauno tehnoloģiju apakšgrupas ziņojumu⁵⁹, lai atvieglotu pierādīšanas pienākumu personām, kas cietušas no mākslīgā intelekta radīta kaitējuma, varētu apsvērt nacionālajos tiesību aktos izdarīt pielāgojumus. Piemēram, pierādīšanas pienākumu varētu saistīt ar (attiecīgā operatora) atbildību konkrētiem tiesību aktos noteiktiem kiberdrošības vai citiem drošības pienākumiem: ja kāds nenodrošina atbildību šiem noteikumiem, varētu mainīt pierādīšanas pienākumu attiecībā uz vainu un cēloņsakarību.

Komisija vēlas uzzināt viedokļus par to, vai un cik lielā mērā varētu būt nepieciešams ar atbilstošas ES iniciatīvas palīdzību mazināt sarežģītības radītās sekas, proti, atvieglot/apvērst

⁵⁹ Ziņojums “Liability for Artificial Intelligence and other emerging technologies”, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

pierādīšanas pienākumu, ko paredz nacionālie noteikumi par atbildību par kaitējumu, ko radījusi mākslīgā intelekta lietotņu darbība.

Ja runā par Savienības tiesību aktiem, saskaņā ar Produktatbildības direktīvu produkts, kas neatbilst obligātajiem drošuma noteikumiem, tiktu uzskatīts par defektīvu neatkarīgi no ražotāja vainas. Tomēr var būt arī iemesli apsvērt veidus, kā cietušajiem atvieglot direktīvā noteikto pierādīšanas pienākumu, jo direktīvas īstenošana balstās uz nacionālajiem noteikumiem par pierādījumiem un cēloņsakarības noteikšanu.

Savienojamība un atvērtība. Pašlaik nav pilnīgi skaidrs, ko drošuma aspektā varētu sagaidīt gadījumos, kad noticis kaitējums, ko radījuši kiberdrošības pārkāpumi saistībā ar produktu, un vai šāds kaitējums tiktu pienācīgi kompensēts saskaņā ar Produktatbildības direktīvu.

Kiberdrošības trūkumi var pastāvēt jau no paša sākuma, kad produkts tiek laists apritē, bet tie var parādīties arī vēlākā posmā, proti, labu laiku pēc produkta laišanas apritē.

Ja atbildības sistēma ir balstīta uz vainu, tad skaidru kiberdrošības pienākumu noteikšana ļauj operatoriem saprast, kas tiem jādara, lai izvairītos no atbildības sekām.

Produktatbildības direktīvas kontekstā varētu aktualizēties jautājums par to, vai, ņemot vērā produkta saprātīgi paredzamo lietojumu, ražotājs būtu varējis paredzēt konkrētas izmaiņas. Piemēram, varētu biežāk tikt piemērots princips “aizstāvība pret vēlāku defektu”, kas nozīmē, ka, ja laikā, kad produkts tika laists apgrozībā, defekts nepastāvēja, ražotājam atbildība nav jāuzņemas, vai princips “aizstāvība pret izstrādes risku” (kas paredz, ka konkrētā brīža zināšanas par tehnikas sasniegumiem defektu neļāva paredzēt). Turklāt atbildību varētu samazināt, ja cietusī persona nav veikusi drošumam relevantos atjauninājumus. To, iespējams, varētu uzskatīt par cietušās personas līdznolaidību, un tas tādējādi varētu samazināt ražotāja atbildību. Tā kā var aktualizēties jēdziens “paredzams saprātīgs izmantojums” un jautājumi par līdznolaidību (tā ir, piemēram, drošuma atjauninājumu neiejuplādēšana), cietušajām personām var būt grūtāk saņemt kompensāciju par kaitējumu, ko izraisījis produkta defekts.

Autonomija un necaurredzamība. Ja mākslīgais intelekts spēj darboties autonomi, tam uzdevuma izpildei nav vajadzīgs, lai katrs solis būtu iepriekšdefinēts, un tam ir vajadzīga ļoti neliela tieša cilvēka vadība vai uzraudzība vai tāda nav vajadzīga vispār. Saprast algoritmus, kuru pamatā ir mašīnmācīšanās, var būt grūti vai pat neiespējami (t. s. “melnās kastes efekts”).

Tāpēc saņemt kompensāciju par autonomu MI lietotņu nodarīto kaitējumu var būt grūti ne tikai iepriekš aprakstītās sarežģītības, bet arī “melnās kastes efekta” dēļ. Algoritma un MI izmantoto datu izprašanai ir vajadzīgas analītiskas spējas un tehniskās zināšanas, kas cietušajiem varētu izrādīties par dārgu. Turklāt, ja potenciāli atbildīgā puse atsakās sadarboties, piekļūt algoritmam un datiem varētu būt neiespējami. Tādējādi praksē cietušie var nebūt spējīgi celt prasību par atbildību. Turklāt nebūtu skaidrs, kā pierādīt tāda MI vainu, kas darbojas autonomi, vai kas būtu uzskatāms par tādas personas vainu, kura paļaujas uz MI izmantošanu.

Nacionālajos tiesību aktos jau ir izstrādāti vairāki risinājumi, kā līdzīgās situācijās cietušajiem samazināt pierādīšanas pienākumu.

Savienības produktu drošuma un produktatbildības aktu pamatprincips joprojām ir, ka tas ir ražotāja pienākums nodrošināt, ka visi tirgū laistie produkti ir droši visā to aprites ciklā, kā arī attiecībā uz saprātīgi paredzamo produkta izmantošanu. Tas nozīmē, ka ražotājam būtu jāpārlicinās, ka produkts, kurā izmanto MI, atbilst konkrētiem drošuma parametriem.

Mākslīgā intelekta funkcijas neizslēdz tiesības sagaidīt, ka produkts ir drošs, neatkarīgi no tā, vai runa ir par automātisko zāliena pļaujmašīnu vai ķirurģisko robotu.

Autonomija produkta drošumu var ietekmēt, jo tā var būtiski mainīt produkta īpašības, tostarp tā drošuma funkcijas. Jautājums ir par to, ar kādiem nosacījumiem pašmācības funkcijas pagarina ražotāja atbildību un kādā mērā ražotājam dažas izmaiņas būtu vajadzējis paredzēt.

Lai ņemtu vērā to, ka produkti var mainīties un tikt mainīti, varētu pārskatīt jēdzienu “laišana aprītē”, ko pašlaik lieto Produktatbildības direktīvā, un tas jādara ciešā koordinācijā ar attiecīgajām izmaiņām Savienības drošuma regulējumā. Tas varētu arī palīdzēt skaidrot, kurš ir atbildīgs par jebkādam produktā veiktām izmaiņām.

Saskaņā ar Atbildības un jauno tehnoloģiju ekspertu grupas Jauno tehnoloģiju apakšgrupas ziņojumu⁶⁰, dažu autonomu MI ierīču un pakalpojumu darbībai varētu būt īpašs riska profils atbildības ziņā, jo tās var nodarīt būtisku kaitējumu svarīgām likumīgām interesēm, piemēram, dzīvībai, veselībai un īpašumam, un pakļaut riskam plašu sabiedrību. Tas galvenokārt varētu attiekties uz MI ierīcēm, kas pārvietojas sabiedriskās vietās (piemēram, pilnīgi autonomi transportlīdzekļi, bezpilota lidaparāti⁶¹ un paciņu piegādes roboti), vai uz MI balstītiem pakalpojumiem ar līdzīgu risku (piemēram, satiksmes pārvaldības pakalpojumi, kas virza vai kontrolē transportlīdzekļus, vai elektroenerģijas sadales pārvaldība). Problēmas, ko autonomija un necaurredzamība rada nacionālajās deliktu tiesībās, varētu risināt, izmantojot uz risku balstītu pieeju. Shēmas, kas paredz atbildību neatkarīgi no vainas, varētu nodrošināt, ka ikreiz, kad šis risks materializējas, cietušais saņem kompensāciju neatkarīgi no vainas. Rūpīgi jāizvērtē, kā MI izstrādi un plašāku ieviešanu ietekmēs tas, kura persona tiks izvēlēta par atbildīgo neatkarīgi no vainas, un jāapsver uz risku balstīta pieeja.

Runājot par MI lietojumiem ar īpašu riska profilu, Komisija vēlas noskaidrot viedokļus šādā jautājumā: lai panāktu, ka iespējamie cietušie patiesi saņem kompensāciju, vai un cik lielā mērā vajadzētu ieviest principu par atbildību neatkarīgi no vainas, kurš jau ieviests nacionālajos tiesību aktos, kas attiecas uz līdzīgiem riskiem, kuriem ir pakļauta sabiedrība (piemēram, mehānisko transportlīdzekļu, lidmašīnu vai kodolelektrostaciju ekspluatācijas rezultātā). Komisija arī vēlas uzzināt viedokļus par to, ka atbildību neatkarīgi no vainas varētu apvienot ar iespējamu pienākumu iegādāties pieejamo apdrošināšanu, par paraugu ņemot Mehānisko transportlīdzekļu apdrošināšanas direktīvu; tādējādi tiktu nodrošināta kompensācija neatkarīgi no atbildīgās personas maksātspējas, un tas palīdzētu samazināt kaitējuma izmaksas.

Attiecībā uz visu pārējo MI lietotņu darbību, kas veidotu lielāko daļu MI lietotņu, Komisija ir pārdomās par to, vai vajadzētu pielāgot pierādīšanas pienākumu attiecībā uz cēloņsakarību un vainu. Šajā sakarā viens no problēmjautājumiem, kas atzīmēts Atbildības un jauno tehnoloģiju ekspertu grupas Jauno tehnoloģiju apakšgrupas ziņojumā⁶², ir situācija, kad potenciāli atbildīgā puse nav reģistrējusi datus, kas ir būtiski atbildības novērtēšanai, vai nevēlas tos kopīgot ar cietušo.

⁶⁰ Ziņojums “Liability for Artificial Intelligence and other emerging technologies”, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

⁶¹ Sal. ar bezpilota gaisa kuģu sistēmām, kas minētas Komisijas Īstenošanas regulā (ES) 2019/947 (2019. gada 24. maijs) par bezpilota gaisa kuģu ekspluatācijas noteikumiem un procedūrām.

⁶² Ziņojums “Liability for Artificial Intelligence and other emerging technologies”, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

4. Secinājumi

Tādu jaunu digitālo tehnoloģiju parādīšanās kā mākslīgais intelekts, lietu internets un robotika rada jaunas problēmas saistībā ar produktu drošumu un atbildību; problēmas rada, piemēram, savienojamība, autonomija, datatkarība, necaurredzamība, produktu un sistēmu sarežģītība, programmatūras atjauninājumi un sarežģītākas drošuma pārvaldības un vērtību ķēdes.

Pašreizējos produktu drošuma tiesību aktos, jo īpaši Produktu vispārējā drošuma direktīvā, Mašīnu direktīvā, Radioiekārtu direktīvā un jaunajā tiesiskajā regulējumā, ir vairākas nepilnības, kas jānovērš. Turpmākais darbs pie dažādu tiesību aktu pielāgošanas šajā satvarā tiks veikts konsekventi un saskaņoti.

Jaunās problēmas drošuma aspektā rada arī jaunas problēmas atbildības aspektā. Šīs ar atbildību saistītās problēmas ir jārisina, lai garantētu tādu pašu aizsardzības līmeni kā personām, kas cietušas no tradicionālajām tehnoloģijām, taču vienlaikus jā saglabā līdzsvars ar tehnoloģisko inovāciju vajadzībām. Tas palīdzēs vairost uzticēšanos šīm jaunajām digitālajām tehnoloģijām un dos stabilitāti investoriem.

Lai gan principā Savienības un valstu tiesību akti, kas pašreiz ir spēkā atbildības jomā, jauno tehnoloģiju sakarā radušās problēmas spēj risināt, MI problēmu apmērs un kopējā ietekme varētu radīt grūtības piedāvāt kompensāciju cietušajiem visos gadījumos, kad tas būtu pamatoti⁶³. Tādējādi izmaksu sadalījums saskaņā ar spēkā esošajiem noteikumiem kaitējuma gadījumā var izrādīties netaisnīgs vai neefektīvs. Lai to labotu un novērstu iespējamās neskaidrības esošajā regulējumā, varētu apsvērt ar atbilstošu ES iniciatīvu palīdzību Produktatbildības direktīvā un nacionālajos atbildības jomas režīmos veikt dažus pielāgojumus, tam izmantojot mērķorientētu, uz risku balstītu pieeju, t. i., ņemot vērā to, ka dažādi MI lietojumi rada atšķirīgus riskus.

⁶³ Sk. Jauno tehnoloģiju apakšgrupas ziņojuma 3. lpp. un Mākslīgā intelekta augsta līmeņa ekspertu grupas rīcībpolitisko ieteikumu Nr. 27.2.