

Bruxelles, 19.2.2020.
COM(2020) 64 final

**IZVJEŠĆE KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU I EUROPSKOM
GOSPODARSKOM I SOCIJALNOM ODBORU**

**Izvješće o utjecaju umjetne inteligencije, interneta stvari i robotike na sigurnost i
odgovornost**

IZVJEŠĆE O UTJECAJU UMJETNE INTELIGENCIJE, INTERNETA STVARI I ROBOTIKE NA SIGURNOST I ODGOVORNOST

1. Uvod

Umjetna inteligencija (UI)¹, internet stvari² i robotika stvorit će nove prilike i koristi za naše društvo. Komisija je prepoznala važnost i potencijal tih tehnologija te potrebu za znatnim ulaganjima u tim područjima.³ Zalaže se za to da Europa postane svjetski predvodnik u području umjetne inteligencije, interneta stvari i robotike. Kako bi se postigao taj cilj, potreban je jasan i predvidljiv pravni okvir za odgovor na tehnološke izazove.

1.1. Postojeći okvir za sigurnost i odgovornost

Opći je cilj pravnih okvira za sigurnost i odgovornost siguran, pouzdan i dosljedan rad svih proizvoda i usluga, uključujući one koji integriraju perspektivne digitalne tehnologije, te učinkovito otklanjanje nastale štete. Visoke razine sigurnosti proizvoda i sustava koji koriste nove digitalne tehnologije i čvrsti mehanizmi za otklanjanje nastale štete (tj. okvir za odgovornost) pridonose boljoj zaštiti potrošača. Usto, njima se gradi povjerenje u te tehnologije, što je preduvjet kako bi ih industrija i korisnici primjenjivali. Time će se pak povećati konkurentnost naše industrije i pridonijeti ciljevima Unije⁴. Jasan okvir za sigurnost i odgovornost još je važniji kako bi se zaštitili potrošači i poduzećima zajamčila pravna sigurnost kada se pojave nove tehnologije kao što su umjetna inteligencija, internet stvari i robotika.

Unija ima čvrst i pouzdan regulatorni okvir za sigurnost i odgovornost za proizvode te čvrst korpus sigurnosnih normi, dopunjen nacionalnim, neusklađenim zakonodavstvom o odgovornosti. Njima se osigurava dobrobit naših građana na jedinstvenom tržištu te potiču inovacije i primjena novih tehnologija. Međutim, umjetna inteligencija, internet stvari i robotika mijenjaju karakteristike mnogih proizvoda i usluga.

U Komunikaciji o umjetnoj inteligenciji za Europu⁵, donesenoj 25. travnja 2018., najavljeno je da će Komisija podnijeti izvješće o procjeni značenja novih digitalnih tehnologija u postojećim okvirima za sigurnost i odgovornost. Cilj je ovog Izvješća utvrditi i ispitati šire značenje i potencijalne nedostatke u okvirima odgovornosti i sigurnosti za umjetnu inteligenciju, internet stvari i robotiku. Smjernice iz ovog Izvješća uz Bijelu knjigu o umjetnoj inteligenciji uzimaju se u obzir u raspravi i dio su šireg savjetovanja s dionicima. Odjeljak o sigurnosti temelji se na evaluaciji⁶ Direktive o strojevima⁷ i radu s relevantnim

¹ Stručna skupina na visokoj razini (AI HLEG) definira umjetnu inteligenciju ovdje: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>

² Definicija interneta stvari iz Preporuke ITU-T Y.2060 dostupna je na <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>

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

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

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

Popratni radni dokument službi Komisije (2018) 137 (<https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137>) sadržava prvi pregled izazova povezanih s odgovornošću koji se pojavljuju u kontekstu perspektivnih digitalnih tehnologija.

⁶ SWD(2018) 161 final.

⁷ Direktiva 2006/42/EZ.

stručnim skupinama⁸. Odjeljak o odgovornosti temelji se na evaluaciji⁹ Direktive o odgovornosti za proizvode¹⁰, doprinosu relevantnih stručnih skupina¹¹ i komunikaciji s dionicima. Ovim se Izvješćem ne nastoji pružiti iscrpan pregled postojećih pravila o sigurnosti i odgovornosti, već je usmjereno na do sada utvrđena ključna pitanja.

1.2. Karakteristike tehnologija umjetne inteligencije, interneta stvari i robotike

Umjetna inteligencija, internet stvari i robotika dijele mnoge karakteristike. Mogu kombinirati **povezivost**, **autonomiju** i **ovisnost o podacima** kako bi obavljali zadaće uz malu ili nikakvu ljudsku kontrolu ili nadzor. Sustavi opremljeni umjetnom inteligencijom mogu povećati svoju uspješnost i učenjem iz iskustva. Njihova se **složenost** odražava u nizu gospodarskih subjekata uključenih u **lanac opskrbe** i u mnoštvu komponenata, dijelova, softvera, sustava ili usluga, koji zajedno čine nove tehnološke ekosustave. Tu je i **otvorenost** za ažuriranje i nadogradnju nakon njihova stavljanja na tržište. Goleme količine podataka, oslanjanje na algoritme i **netransparentnost** donošenja odluka umjetne inteligencije otežavaju predviđanje ponašanja proizvoda omogućenog umjetnom inteligencijom i razumijevanje mogućih uzroka štete. Naposljetku, povezivost i otvorenost mogu proizvode umjetne inteligencije i interneta stvari izložiti i **kiberprijetnjama**.

1.3. Mogućnosti koje stvaraju umjetna inteligencija, internet stvari i robotika

Veće povjerenje korisnika i društvena prihvaćenost perspektivnih tehnologija, bolji proizvodi, procesi i poslovni modeli te pomoć europskim proizvođačima da postanu učinkovitiji samo su neke od mogućnosti koje pružaju umjetna inteligencija, internet stvari i robotika.

Osim veće produktivnosti i učinkovitosti, umjetna inteligencija ljudima obećava razvoj dosad nezamislive inteligencije, otvarajući vrata novim otkrićima i pomažući u rješavanju nekih od najvećih svjetskih problema: od liječenja kroničnih bolesti, predviđanja izbijanja bolesti ili smanjenja stope smrtnih slučajeva u prometnim nesrećama do borbe protiv klimatskih promjena ili predviđanja kiberprijetnji.

Te tehnologije mogu donijeti brojne koristi povećanjem sigurnosti proizvoda, zbog čega postaju manje podložni određenim rizicima. Na primjer, povezana i automatizirana vozila mogla bi povećati sigurnost na cestama jer je većina prometnih nesreća trenutačno uzrokovana ljudskim pogreškama¹². Nadalje, sustavi interneta stvari projektirani su za

⁸ Mreža za sigurnost potrošača kako je uspostavljena Direktivom 2001/95/EZ o općoj sigurnosti proizvoda, Direktivom 2006/42/EZ o strojevima i Direktivom o radijskoj opremi 2014/53/EU, stručne skupine dionika iz država članica i industrije te drugih dionika kao što su udruge potrošača.

⁹ COM(2018) 246 final.

¹⁰ Direktiva 85/374/EEZ.

¹¹ Stručna skupina za odgovornost i nove tehnologije osnovana je kako bi Komisiji pružila stručno znanje o primjenjivosti Direktive o odgovornosti za proizvode i nacionalnih pravila o građanskopravnoj odgovornosti te pomoć u razvoju vodećih načela za moguće prilagodbe primjenjivih zakona povezanih s novim tehnologijama. Sastoji se od dviju podskupina – podskupine za odgovornost za proizvode i podskupine za nove tehnologije, vidjeti <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1>.

Za Izvješće podskupine za nove tehnologije o odgovornosti za umjetnu inteligenciju i druge perspektivne tehnologije vidjeti https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

¹² Procjenjuje se da približno 90 % prometnih nezgoda nastaje zbog ljudske pogreške. Vidjeti izvješće Komisije „Spašavanje života: poboljšanje sigurnosti automobila u EU-u” (COM(2016) 0787 final).

primanje i obradu velikih količina podataka iz različitih izvora. Ta viša razina informacija mogla bi se upotrijebiti kako bi se proizvodi mogli sami prilagoditi i time postati sigurniji. Nove tehnologije mogu doprinijeti djelotvornosti opoziva proizvoda jer bi, na primjer, proizvodi mogli upozoriti korisnike radi izbjegavanja sigurnosnog problema¹³. Ako se tijekom uporabe povezanog proizvoda pojavi sigurnosni problem, proizvođači mogu izravno komunicirati s korisnicima, s jedne strane, kako bi ih upozorili na rizike i, s druge strane, ako je to moguće, kako bi izravno riješili problem, primjerice, sigurnosnim ažuriranjem. Na primjer, pri opozivu jednog od svojih uređaja 2017. proizvođač pametnih telefona ažurirao je softver kako bi se kapacitet baterija opozvanih telefona¹⁴ smanjio na nulu te korisnici tako prestali upotrebljavati opasne uređaje.

Nadalje, nove tehnologije mogu pridonijeti boljoj sljedivosti proizvoda. Primjerice, značajke povezivosti interneta stvari mogu poduzećima i tijelima za nadzor tržišta omogućiti praćenje opasnih proizvoda i utvrđivanje rizika u svim lancima opskrbe¹⁵.

Uz mogućnosti koje umjetna inteligencija, internet stvari i robotika mogu donijeti gospodarstvu i našim društvima, oni mogu i stvoriti rizik od nanošenja štete pravno zaštićenim materijalnim i nematerijalnim interesima. Rizik od nastanka takve štete povećat će se usporedno s područjem uporabe tih tehnologija. U tom je kontekstu ključno analizirati je li i u kojoj mjeri postojeći pravni okvir za sigurnost i odgovornost i dalje prikladan za zaštitu korisnika.

2. Sigurnost

U komunikaciji Komisije „Izgradnja povjerenja u antropocentričnu umjetnu inteligenciju” navodi se: „**sustavi umjetne inteligencije trebali bi uključivati integrirane sigurnosne mehanizme kako bi se osiguralo da se njihova sigurnost može provjeriti u svakoj fazi**, pri čemu treba uzeti u obzir **fizičku i mentalnu sigurnost** svih zainteresiranih strana¹⁶”.

Procjenom zakonodavstva Unije o sigurnosti proizvoda u ovom odjeljku analizira se sadržava li postojeći zakonodavni okvir Unije relevantne elemente kako bi se osiguralo da perspektivne tehnologije, a posebno UI sustavi, uključuju sigurnost upotrebe i integriranu sigurnost.

U ovom se Izvješću uglavnom razmatra Direktiva o općoj sigurnosti proizvoda¹⁷ i usklađeno zakonodavstvo o proizvodima koje slijedi horizontalna pravila „novog pristupa”¹⁸ i/ili „novog zakonodavnog okvira” (dalje u tekstu „zakonodavstvo Unije o sigurnosti proizvoda ili okvir

¹³ Na primjer, vozač automobila može primiti upozorenje da uspori u slučaju da se kreće prema mjestu nesreće.

¹⁴ OECD (2018.), *Measuring and maximising the impact of product recalls globally*:

OECD workshop report, (Mjerenje i maksimalno povećanje učinka opoziva proizvoda na svjetskoj razini: izvješće OECD-a s radionice), *OECD Science, Technology and Industry Policy Papers*, br. 56, OECD Publishing, Pariz, <https://doi.org/10.1787/ab757416-en>.

¹⁵ OECD (2018.), *Enhancing product recall effectiveness globally: OECD background report* (Poboljšanje globalne učinkovitosti opoziva proizvoda: popratno izvješće OECD-a), *OECD Science, Technology and Industry Policy Papers*, br. 58, OECD Publishing, Pariz, <https://doi.org/10.1787/ef71935c-en>

¹⁶ Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija o izgradnji povjerenja u antropocentričnu umjetnu inteligenciju, Bruxelles, 8.4.2019., COM(2019) 168 final.

¹⁷ Direktiva 2001/95/EZ Europskog parlamenta i Vijeća od 3. prosinca 2001. o općoj sigurnosti proizvoda (SL L 11, 15.1.2002., str. 4.–17.).

¹⁸ SL C 136, 4.6.1985., str. 1.

Unije za sigurnost proizvoda”)¹⁹. Horizontalna pravila osiguravaju usklađenost sektorskih pravila o sigurnosti proizvoda.

Zakonodavstvom Unije o sigurnosti proizvoda nastoji se osigurati da proizvodi koji se stavljaju na tržište Unije ispunjavaju visoke zdravstvene i sigurnosne zahtjeve, kao i zahtjeve za zaštitu okoliša, te da takvi proizvodi mogu slobodno biti u optjecaju na tržištu u cijeloj Uniji. Sektorsko zakonodavstvo²⁰ dopunjeno je Direktivom o općoj sigurnosti proizvoda²¹, kojom se zahtijeva da svi potrošački proizvodi, čak i ako nisu uređeni sektorskim zakonodavstvom Unije, moraju biti sigurni. Sigurnosna pravila nadopunjuju se nadzorom tržišta i ovlastima dodijeljenima nacionalnim tijelima u skladu s Uredbom o nadzoru tržišta²² i Direktivom o općoj sigurnosti proizvoda²³. U prijevozu postoje dodatna pravila Unije i nacionalna pravila za stavljanje u promet motornog vozila²⁴, zrakoplova ili broda te jasna pravila kojima se uređuje sigurnost tijekom rada, uključujući zadaće operatera i zadaće nadzora nadležnih tijela.

Među ključnim je elementima zakonodavstva Unije o sigurnosti proizvoda i europska normizacija. S obzirom na globalnu prirodu digitalizacije i perspektivnih digitalnih tehnologija, međunarodna suradnja u području normizacije posebno je važna za konkurentnost europske industrije.

Velik dio okvira Unije za sigurnost proizvoda izrađen je prije pojave digitalnih tehnologija kao što su umjetna inteligencija, internet stvari ili robotika. Stoga taj okvir ne sadržava uvijek odredbe koje se izričito odnose na nove izazove i rizike tih perspektivnih tehnologija. Međutim, premda je postojeći okvir za sigurnost proizvoda tehnološki neutralan, to ne znači da se ne bi primjenjivao na proizvode u koje su ugrađene te tehnologije. Nadalje, u naknadnim zakonodavnim aktima koji su dio tog okvira, primjerice u sektoru medicinskih proizvoda ili automobila, već su se izričito razmatrali neki aspekti perspektivnih digitalnih tehnologija, npr. automatizirane odluke, softver kao zaseban proizvod i povezivost.

¹⁹ Uredba (EZ) br. 2008/765 i Odluka (EZ) br. 2008/768.

²⁰ Ta shema ne uključuje zakonodavstvo Unije o prijevozu i automobilima.

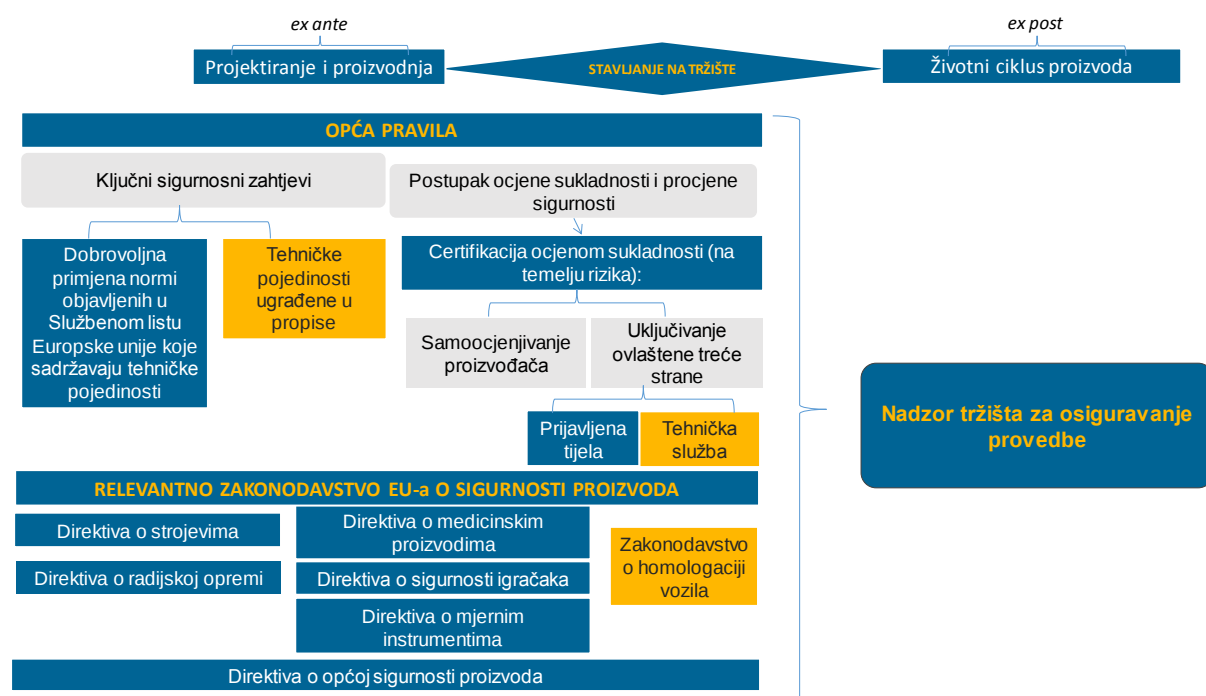
²¹ Direktiva 2001/95/EZ Europskog parlamenta i Vijeća od 3. prosinca 2001. o općoj sigurnosti proizvoda (SL L 11, 15.1.2002., str. 4.–17.).

²² Uredba (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93, SL L 218, 13.8.2008., str. 30.–47., ELI: <http://data.europa.eu/eli/reg/2008/765/oj>, i od 2021. Uredba (EU) 2019/1020 Europskog parlamenta i Vijeća od 20. lipnja 2019. o nadzoru tržišta i sukladnosti proizvoda i o izmjeni Direktive 2004/42/EZ i uredbi (EZ) br. 765/2008 i (EU) br. 305/2011, SL L 169, 25.6.2019., str. 1.–44., ELI: <http://data.europa.eu/eli/reg/2019/1020/oj>

²³ Članak 8. stavak 1. točka (b) podtočka 3. Direktive o općoj sigurnosti proizvoda.

²⁴ Na primjer, Direktiva 2007/46/EZ – homologacija motornih vozila i njihovih prikolica te sustava, sastavnih dijelova i zasebnih tehničkih jedinica namijenjenih za takva vozila i Uredba (EU) 2018/858 Europskog parlamenta i Vijeća od 30. svibnja 2018. o homologaciji i nadzoru tržišta motornih vozila i njihovih prikolica te sustavâ, sastavnih dijelova i zasebnih tehničkih jedinica namijenjenih za takva vozila, o izmjeni uredbi (EZ) br. 715/2007 i (EZ) br. 595/2009 te o stavljanju izvan snage Direktive 2007/46/EZ.

Temeljna logika postojećeg zakonodavstva Unije o sigurnosti proizvoda²⁵



Dalje u tekstu opisani su izazovi koje perspektivne digitalne tehnologije donose za okvir Unije za sigurnost proizvoda.

Povezivost je ključna značajka sve većeg broja proizvoda i usluga. Ta značajka dovodi u pitanje tradicionalni koncept sigurnosti jer povezivost može izravno ugroziti sigurnost proizvoda, a neizravno, ako se hakira, može dovesti do sigurnosnih prijetnji i utjecati na sigurnost korisnikâ.

Primjer je obavijest sustava brzog uzbuđivanja EU-a iz Islanda o pametnom satu za djecu²⁶. Taj proizvod ne bi prouzročio izravnu štetu djetetu koje ga nosi, ali s obzirom na to da mu nedostaje minimalna razina sigurnosti, lako se može upotrijebiti kao alat za pristup djetetu. Budući da je jedna od predviđenih funkcija proizvoda sigurnost djece određivanjem njihove lokacije, potrošač ne očekuje da bi sat mogao predstavljati sigurnosnu prijetnju, tj. da bi dijete svatko mogao pratiti i/ili s njim kontaktirati.

Drugi je primjer naveden u obavijesti koju je dostavila Njemačka u vezi s osobnim automobilom²⁷. Radio u vozilu može imati određene softverske sigurnosne nedostatke koji trećim osobama omogućuju neovlašteni pristup međusobno povezanim upravljačkim sustavima u vozilu. Kad bi treća osoba iskoristila te softverske sigurnosne nedostatke u zlonamjerne svrhe, mogla bi se dogoditi nesreća na cesti.

Ako industrijske aplikacije nisu dovoljno sigurne, mogu biti izložene i kiberprijetnjama koje utječu na sigurnost osoba u većim razmjerima. To se može dogoditi, na primjer, u slučaju kibernetičke napada na ključni sustav kontrole industrijskog postrojenja namijenjenog za pokretanje potencijalno smrtonosne eksplozije.

²⁵ Ova slika ne uključuje zahtjeve zakonodavstva koji se odnose na životni ciklus proizvoda, tj. uporabu i održavanje, te je prikazana samo u opće ilustracijske svrhe.

²⁶ Obavijest Islanda u sustavu RAPEX objavljena na internetskoj stranici EU Safety Gate (A12/0157/19).

²⁷ Obavijest Njemačke u sustavu RAPEX objavljena na internetskoj stranici EU Safety Gate (A12/1671/15).

Zakonodavstvom Unije o sigurnosti proizvoda općenito se ne predviđaju posebni obvezni osnovni zahtjevi protiv kiberprijetnji koje utječu na sigurnost korisnika. Međutim, odredbe o sigurnosnim aspektima sadržane su u Uredbi o medicinskim proizvodima²⁸, Direktivi o mjernim instrumentima²⁹, Direktivi o radijskoj opremi³⁰ i zakonodavstvu o homologaciji vozila³¹. Aktom o kibersigurnosti³² uspostavlja se dobrovoljni okvir za kibersigurnosnu certifikaciju za proizvode, usluge i procese informacijske i komunikacijske tehnologije (IKT), dok se u relevantnom zakonodavstvu Unije o sigurnosti proizvoda utvrđuju obvezni zahtjevi.

Osim toga, rizik od gubitka povezivosti perspektivnih digitalnih tehnologija može uključivati i rizike povezane sa sigurnošću. Na primjer, ako povezani protupožarni alarm izgubi povezivost, možda neće upozoriti korisnika u slučaju požara.

Sigurnost u postojećem zakonodavstvu Unije o sigurnosti proizvoda cilj je javne politike. Koncept sigurnosti povezan je s uporabom proizvoda i rizicima, npr. mehaničkim, električnim itd., koje treba riješiti kako bi proizvod bio siguran. Treba napomenuti da, ovisno o zakonodavstvu Unije koje se odnosi na sigurnost proizvoda, uporaba proizvoda ne obuhvaća samo predviđenu namjenu nego i predviđivu uporabu, a u nekim slučajevima, kao što je Direktiva o strojevima³³, čak i razumno predviđivu nepravilnu uporabu.

Koncept sigurnosti u postojećem zakonodavstvu Unije o sigurnosti proizvoda u skladu je s proširenim konceptom sigurnosti kako bi se zaštitili potrošači i korisnici. Stoga koncept sigurnosti proizvoda obuhvaća zaštitu od svih vrsta rizika koji proizlaze iz proizvoda, ne samo mehaničkih, kemijskih i električnih, nego i kiberrizika i rizika povezanih s gubitkom povezivosti proizvoda.

Izričite odredbe u tom pogledu mogle bi se razmotriti za područje primjene relevantnih zakonodavnih akata Unije kako bi se korisnici bolje zaštitili, a pravna sigurnost povećala.

Autonomija³⁴ je jedna od glavnih značajki umjetne inteligencije. Nenamjerni ishodi dobiveni umjetnom inteligencijom mogli bi naštetiti korisnicima i izloženim osobama.

U mjeri u kojoj se buduće „ponašanje” proizvoda umjetne inteligencije može unaprijed utvrditi na temelju procjene rizika koju provodi proizvođač prije stavljanja proizvoda na tržište, okvirom Unije za sigurnost proizvoda već se utvrđuju obveze proizvođača da pri procjeni rizika uzmu u obzir „uporabu”³⁵ proizvoda tijekom njihova radnog vijeka. Usto, proizvođače se obvezuje da korisnike opskrbe uputama i podacima o sigurnosti ili ih upozore na sigurnosna pitanja³⁶. U tom se kontekstu, na primjer, u Direktivi o radijskoj opremi³⁷ od

²⁸ Uredba (EU) 2017/745 o medicinskim proizvodima.

²⁹ Direktiva 2014/32/EU o stavljanju na raspolaganje mjernih instrumenata na tržištu.

³⁰ Direktiva o radijskoj opremi 2014/53/EU.

³¹ Direktiva 2007/46/EZ – homologacija motornih vozila i njihovih prikolica te sustava, sastavnih dijelova i zasebnih tehničkih jedinica namijenjenih za takva vozila. Direktiva će s učinkom od 1. rujna 2020. biti stavljena izvan snage i zamijenjena Uredbom (EU) 2018/858 o homologaciji i nadzoru tržišta motornih vozila i njihovih prikolica te sustavâ, sastavnih dijelova i zasebnih tehničkih jedinica namijenjenih za takva vozila, o izmjeni uredaba (EZ) br. 715/2007 i (EZ) br. 595/2009 te o stavljanju izvan snage Direktive 2007/46/EZ.

³² Uredba (EU) 2019/881.

³³ Direktiva 2006/42/EZ o strojevima.

³⁴ Iako proizvodi koji se temelje na umjetnoj inteligenciji mogu djelovati autonomno promatranjem svojeg okruženja i bez skupa unaprijed utvrđenih uputa, njihovo je ponašanje ograničeno ciljem koji im se zadaje i drugim relevantnim odrednicama za koje se odluče njihovi programeri.

³⁵ U zakonodavstvu Unije o sigurnosti proizvoda proizvođači procjenu rizika temelje na predviđenoj uporabi proizvoda, predviđivoj uporabi i/ili razumno predviđivoj nepravilnoj uporabi.

³⁶ Odluka br. 768/2008/EZ Europskog parlamenta i Vijeća od 9. srpnja 2008. o zajedničkom okviru za stavljanje na tržište proizvoda i o stavljanju izvan snage Odluke Vijeća 93/465/EEZ, SL L 218, 13.8.2008., str. 82.–128. Prilog I. članak R2. stavak 7. glasi: „Proizvođači osiguravaju da su uz proizvod priložene upute

proizvođača zahtijeva da uključi upute s informacijama o načinu uporabe radijske opreme u skladu s njezinom namjenom.

U budućnosti se mogu pojaviti i situacije u kojima se ishodi UI sustava ne mogu unaprijed u potpunosti utvrditi. U takvoj situaciji procjena rizika provedena prije stavljanja proizvoda na tržište možda više ne odražava uporabu, funkcioniranje ili ponašanje proizvoda. U tim slučajevima, u mjeri u kojoj je uporaba koju je prvotno predvidio proizvođač izmijenjena³⁸ zbog autonomnog ponašanja i ugrožavanja sukladnosti sa sigurnosnim zahtjevima, moglo bi se smatrati da je potrebno ponoviti procjenu proizvoda koji samostalno uči³⁹.

U skladu s postojećim okvirom, ako proizvođači saznaju da proizvod tijekom svojeg životnog ciklusa predstavlja rizik koji utječe na sigurnost, dužni su odmah obavijestiti nadležna tijela i poduzeti mjere za sprečavanje rizika za korisnike⁴⁰.

Osim procjene rizika koja se provodi prije stavljanja proizvoda na tržište, mogao bi se uvesti novi postupak procjene rizika ako se proizvod bitno mijenja tijekom radnog vijeka, npr. ako izvršava drugu funkciju koju proizvođač nije predvidio u početnoj procjeni rizika. Taj bi postupak trebao biti usmjeren na učinak na sigurnost uzrokovan autonomnim ponašanjem tijekom cijelog radnog vijeka proizvoda. Procjenu rizika trebao bi provesti odgovarajući gospodarski subjekt. Osim toga, relevantni zakonodavni akti Unije mogli bi uključivati pojačane zahtjeve za proizvođače u pogledu uputa i upozorenja za korisnike.

Slične procjene rizika već se zahtijevaju u zakonodavstvu o prijevozu⁴¹; na primjer, u zakonodavstvu o željezničkom prijevozu, ako se željezničko vozilo mijenja nakon izdavanja potvrde, onaj tko provodi izmjenu mora pokrenuti poseban postupak s jasno utvrđenim kriterijima kako bi se utvrdilo je li potrebno uključiti nadležno tijelo.

Značajka samoučenja proizvoda i sustava umjetne inteligencije može omogućiti uređaju donošenje odluka koje odstupaju od onoga što su mu proizvođači prvotno namijenili, a time i od onoga što korisnici očekuju. Time se propituje ljudska kontrola jer bi ljudi mogli birati kako će i hoće li delegirati odluku proizvodima i sustavima umjetne inteligencije kako bi se

i podaci o sigurnosti na jeziku koji je lako razumljiv potrošačima i drugim krajnjim korisnicima te na način koji je utvrdila dotična država članica.”

³⁷ Članak 10. stavak 8., koji se odnosi na upute za krajnjeg korisnika, i Prilog VI., koji se odnosi na EU izjavu o sukladnosti.

³⁸ Do sada se „samostalno učenje” u kontekstu umjetne inteligencije uglavnom koristi kako bi se pokazalo da strojevi mogu učiti tijekom treniranja; još nije potrebno da uređaji umjetne inteligencije i dalje uče nakon što se počnu koristiti; naprotiv, osobito u zdravstvu, uređaji umjetne inteligencije obično prestaju učiti nakon uspješnog završetka treniranja. Stoga u ovoj fazi autonomno ponašanje koje proizlazi iz UI sustava ne znači da proizvod obavlja zadaće koje programeri nisu predvidjeli.

³⁹ To je u skladu s odjeljkom 2.1. „Plavog vodiča” o provedbi pravila EU-a o proizvodima 2016.

⁴⁰ Članak 5. Direktive 2001/95/EZ Europskog parlamenta i Vijeća od 3. prosinca 2001. o općoj sigurnosti proizvoda.

⁴¹ U slučaju bilo kakve promjene u željezničkom sustavu koja bi mogla utjecati na sigurnost (npr. tehnička, operativna ili organizacijska promjena koja bi mogla utjecati na operativne postupke ili održavanje), postupak koji treba slijediti opisan je u Prilogu I. Provedbenoj uredbi Komisije (EU) 2015/1136 (SL L 185, 14.7.2015., str. 6.).

U slučaju „značajne promjene” neovisno „tijelo za procjenu” (može biti nacionalno tijelo nadležno za sigurnost ili drugo tehnički nadležno tijelo) trebalo bi dostaviti izvješće o procjeni sigurnosti predlagatelju promjene.

Nakon analize rizika predlagatelj promjene primijenit će odgovarajuće mjere za ublažavanje rizika (ako je predlagatelj željeznički prijevoznik ili upravitelj infrastrukture, primjena Uredbe dio je njegova sustava upravljanja sigurnošću čiju primjenu nadzire nacionalno tijelo nadležno za sigurnost).

postigli ciljevi koje je odabrao čovjek⁴². Postojeće zakonodavstvo Unije o sigurnosti proizvoda ne odnosi se izričito na ljudski nadzor u kontekstu proizvoda i sustava umjetne inteligencije koji samostalno uče⁴³.

Relevantnim zakonodavnim aktima Unije mogu se kao zaštitna mjera predvidjeti posebni zahtjevi za ljudski nadzor, počevši od projektiranja proizvoda pa tijekom cijelog životnog ciklusa proizvoda i sustava umjetne inteligencije.

Buduće „ponašanje” UI aplikacija moglo bi prouzročiti **rizike za mentalno zdravlje**⁴⁴ korisnika koji proizlaze, primjerice, iz njihove suradnje s humanoidnim robotima i sustavima umjetne inteligencije kod kuće ili u radnim okruženjima. U tom se pogledu pod sigurnošću općenito upućuje na prijetnju koju korisnik smatra fizičkom štetom koja može proizaći iz perspektivne digitalne tehnologije. Istodobno, sigurni proizvodi definirani su u pravnom okviru Unije kao proizvodi koji ne predstavljaju nikakav rizik ili predstavljaju samo minimalne rizike za sigurnost i zdravlje ljudi. Usuglašeno je da definicija zdravlja uključuje i fizičku i mentalnu dobrobit. Međutim, rizici za mentalno zdravlje trebali bi biti izričito obuhvaćeni konceptom sigurnosti proizvoda u zakonodavnom okviru.

Na primjer, autonomija ne bi tijekom duljih razdoblja smjela uzrokovati pretjeran stres ni neugodnost ni štetiti mentalnom zdravlju. U tom se pogledu smatra da su čimbenici koji pozitivno utječu na osjećaj sigurnosti za starije osobe⁴⁵ sljedeći: osjećaju se sigurno s osobljem zdravstvene službe, imaju kontrolu nad svakodnevnim radnjama i o njima su informirani. Proizvođači robota koji su u interakciji sa starijim osobama trebali bi uzeti u obzir te čimbenike kako bi se spriječili rizici za mentalno zdravlje.

Za područje primjene relevantnog zakonodavstva EU-a mogle bi se razmotriti izričite obveze proizvođača, među ostalim, humanoidnih robota temeljenih na umjetnoj inteligenciji, da pažljivo razmotre nematerijalnu štetu koju bi njihovi proizvodi mogli uzrokovati korisnicima, naročito ranjivima, kao što su starije osobe u sustavu skrbi.

Još jedna bitna karakteristika proizvoda i sustava koji se temelje na umjetnoj inteligenciji jest **ovisnost o podacima**. Točnost i relevantnost podataka ključne su da bi sustavi i proizvodi koji se temelje na umjetnoj inteligenciji donosili odluke kako je predvidio proizvođač.

Zakonodavstvom Unije o sigurnosti proizvoda nisu izričito obuhvaćeni sigurnosni rizici koji proizlaze iz neispravnih podataka. Međutim, u skladu s „uporabom” proizvoda, proizvođači bi tijekom projektnih i ispitnih faza trebali predvidjeti točnost podataka i njezinu važnost za sigurnosne funkcije.

Na primjer, sustavu koji se temelji na umjetnoj inteligenciji i koji je projektiran za otkrivanje određenih predmeta, može biti teško raspoznavati predmete pri lošoj rasvjeti pa bi projektanti trebali uključiti podatke iz ispitivanja proizvoda u tipičnim i slabo osvijetljenim okruženjima.

⁴² *Policy and Investment Recommendations for Trustworthy AI* (Preporuke za politiku i ulaganja za pouzdanu umjetnu inteligenciju), Stručna skupina na visokoj razini za umjetnu inteligenciju, lipanj 2019.

⁴³ Međutim, to ne isključuje mogućnost da u određenoj situaciji bude potreban nadzor zbog nekih postojećih općenitijih obveza koje se odnose na stavljanje proizvoda na tržište.

⁴⁴ Statut Svjetske zdravstvene organizacije, prva točka: „Zdravlje je stanje potpune fizičke, mentalne i socijalne dobrobiti, a ne samo odsutnost bolesti ili nemoći.” (<https://www.who.int/about/who-we-are/constitution>)

⁴⁵ *Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction* (Socijalni roboti: tehnološki, društveni i etički aspekti interakcije ljudi i robota), str. 237.–264., Neziha Akalin, Annica Kristoffersson i Amy Loutfi, srpanj 2019.

Drugi se primjer odnosi na poljoprivredne robote, kao što su roboti za branje voća čiji je cilj lociranje zrelog voća na stablima ili na tlu. Premda dotični algoritmi već pokazuju stopu uspješnosti razvrstavanja višu od 90 %, nedostatak u skupovima podataka kojima se koriste ti algoritmi može dovesti do toga da ti roboti donesu lošu odluku i, posljedično, ozlijede životinju ili osobu.

Postavlja se pitanje bi li zakonodavstvo EU-a o sigurnosti proizvoda trebalo sadržavati konkretne zahtjeve u pogledu sigurnosnih rizika zbog neispravnih podataka u fazi projektiranja te mehanizme kojima bi se osiguralo održavanje kvalitete podataka tijekom upotrebe proizvoda i sustava umjetne inteligencije.

Netransparentnost je još jedna glavna karakteristika nekih proizvoda i sustava koji se temelje na umjetnoj inteligenciji, a koja može proizaći iz sposobnosti postizanja bolje učinkovitosti učenjem iz iskustva. Ovisno o metodološkom pristupu, proizvodi i sustavi koji se temelje na umjetnoj inteligenciji mogu biti više ili manje netransparentni. To može otežati praćenje postupka odlučivanja sustava (učinak crne kutije (*black-box effect*)). Ljudi možda neće morati razumjeti svaki korak u postupku donošenja odluka, ali s obzirom na to da algoritmi umjetne inteligencije sve više napreduju i primjenjuju se u kritičnim područjima, ključno je da ljudi mogu razumjeti kako su se donijele algoritamske odluke sustava. To bi bilo posebno važno za *ex post* mehanizam provedbe jer bi provedbenim tijelima omogućilo da odrede tko je odgovoran za ponašanje i odabire UI sustava. To je potvrđeno i u Komunikaciji Komisije o izgradnji povjerenja u antropocentričnu umjetnu inteligenciju⁴⁶.

Zakonodavstvom Unije o sigurnosti proizvoda izričito se ne otklanjaju sve veći rizici koji proizlaze iz netransparentnosti sustava koji se temelje na algoritmima. Stoga je potrebno razmotriti zahtjeve za transparentnost algoritama, kao i za pouzdanost, odgovornost i, prema potrebi, ljudski nadzor i nepristrane ishode⁴⁷, što je posebno važno za *ex post* mehanizam provedbe te za izgradnju povjerenja u upotrebu tih tehnologija. Jedan od načina rješavanja tog problema bilo bi uvođenje obveza za programere algoritama da objave parametre projektiranja i metapodatke skupova podataka u slučaju nezgoda.

Dodatni rizici koji mogu utjecati na sigurnost su oni koji proizlaze iz **složenosti proizvoda i sustava** jer se različite komponente, uređaji i proizvodi mogu integrirati i međusobno si utjecati na funkcioniranje (npr. proizvodi koji su dio ekosustava pametnog doma).

Na tu se složenost već odnosi pravni okvir Unije za sigurnost na koji se upućuje na početku ovog odjeljka⁴⁸. Konkretno, kad proizvođač provodi procjenu rizika proizvoda, mora uzeti u obzir predviđenu uporabu, predvidivu uporabu i, prema potrebi, razumno predvidivu nepravilnu uporabu.

U tom kontekstu, **ako proizvođač predvidi da će njegov uređaj biti povezan s drugim uređajima i da će s njima biti u interakciji, to bi trebalo uzeti u obzir tijekom procjene rizika**. Uporaba ili nepravilna uporaba određuje se na temelju, na primjer, iskustva s prošlom uporabom iste vrste proizvoda, istraga nesreća ili ljudskog ponašanja.

Na složenost sustava posebno se odnosi i sektorsko zakonodavstvo o sigurnosti, kao što je Uredba o medicinskim proizvodima, te u određenoj mjeri zakonodavstvo o općoj sigurnosti

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

⁴⁷ Na temelju ključnih zahtjeva koje je predložila stručna skupina na visokoj razini u Etičkim smjernicama za pouzdanu umjetnu inteligenciju: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>

⁴⁸ Uredba (EZ) br. 2008/765 i Odluka (EZ) br. 2008/768 te usklađeno sektorsko zakonodavstvo o sigurnosti proizvoda, npr. Direktiva 2006/42/EZ o strojevima.

proizvoda⁴⁹. Na primjer, proizvođač povezanog uređaja, koji je namijenjen da bude dio ekosustava pametnog doma, trebao bi moći razumno predvidjeti da će njegovi proizvodi utjecati na sigurnost drugih proizvoda.

Uz to, u zakonodavstvu u području prijevoza sustavno se uzima u obzir ta složenost. Za automobile, vlakove i zrakoplove, homologiraju se i certificiraju cijela vozila odnosno zrakoplovi, ali i svi sastavni dijelovi. Cestovna, plovidbena i željeznička interoperabilnost dio su procjene sigurnosti. Ako je riječ o prijevozu, „sustave” mora „odobriti” nadležno tijelo, bilo na temelju ocjene sukladnosti treće strane u odnosu na jasne tehničke zahtjeve, ili nakon što se dokaže kako se otklanjaju rizici. Rješenje je općenito kombinacija razine „proizvoda” i razine „sustava”.

U zakonodavstvu Unije o sigurnosti proizvoda, uključujući zakonodavstvo o prijevozu, već se u određenoj mjeri uzima u obzir složenost proizvoda ili sustava kako bi se uklonili rizici koji mogu utjecati na sigurnost korisnika.

Složeni sustavi često uključuju **softver**, koji je ključna sastavnica sustava koji se temelji na umjetnoj inteligenciji. Općenito, u okviru početne procjene rizika proizvođač konačnog proizvoda ima obvezu predvidjeti rizike softvera ugrađenog u taj proizvod u trenutku njegova stavljanja na tržište.

U određenim dijelovima zakonodavstva Unije o sigurnosti proizvoda izričito se upućuje na softver ugrađen u proizvod. Na primjer, u Direktivi o strojevima⁵⁰ zahtijeva se da nedostatak u programima kontrolnih sustava ne uzrokuje opasne situacije.

U zakonodavstvu Unije o sigurnosti proizvoda ažuriranja softvera mogla bi se izjednačiti s održavanjem iz sigurnosnih razloga pod uvjetom da se njima iz temelja ne mijenja proizvod koji je već stavljen na tržište i da se njima ne uvode novi rizici koji nisu bili predviđeni u početnoj procjeni rizika. Međutim, ako se ažuriranjem softvera taj proizvod iz temelja mijenja, cijeli se može smatrati novim proizvodom, a sukladnost s relevantnim zakonodavstvom o sigurnosti proizvoda mora se ponovno ocijeniti u trenutku provedbe izmjene⁵¹.

Za samostalni softver koji se stavlja na tržište ili učitava nakon što je proizvod stavljen na tržište, usklađeno sektorsko zakonodavstvo Unije o sigurnosti proizvoda općenito ne sadržava posebne odredbe. Međutim, određeni zakonodavni akti Unije odnose se na samostalni softver, primjerice Uredba o medicinskim proizvodima. Nadalje, samostalni softver učitavan u povezane proizvode koji komuniciraju putem određenih radijskih modula⁵² može se regulirati i Direktivom o radijskoj opremi delegiranim aktima. Tom se direktivom zahtijeva da se pri učitavanju softvera ne dovedu u pitanje posebni razredi ili kategorije potpunih funkcija radijske opreme kojima se osigurava da sukladnost te opreme nije ugrožena⁵³.

⁴⁹ U članku 2. Direktive o općoj sigurnosti proizvoda navodi se da se za sigurni proizvod uzima u obzir „utjecaj na druge proizvode u slučaju kad se razumno može predvidjeti da će se on upotrebljavati s drugim proizvodima”.

⁵⁰ Odjeljak 1.2.1. Priloga I. Direktivi o strojevima.

⁵¹ [„Plavi vodič” o provedbi pravila EU-a o proizvodima 2016.](#)

⁵² Radijski moduli su elektronički uređaji koji prenose i/ili primaju radijske signale (WIFI, Bluetooth) između dva uređaja.

⁵³ Članak 3. stavak 3. točka i. Direktive o radijskoj opremi,

Iako se zakonodavstvom Unije o sigurnosti proizvoda uzimaju u obzir sigurnosni rizici koji proizlaze iz softvera ugrađenog u proizvod u trenutku njegova stavljanja na tržište te mogućih naknadnih ažuriranja koja je predvidio proizvođač, mogli bi biti potrebni posebni i/ili izričiti zahtjevi za samostalni softver (npr. aplikacija koja bi se preuzela). Posebno bi trebalo razmotriti samostalni softver kojim se osiguravaju sigurnosne funkcije u proizvodima i sustavima umjetne inteligencije.

Mogle bi biti potrebne dodatne obveze za proizvođače kako bi se osiguralo da taj softver ima značajke kojima se sprečava da njegovo učitavanje utječe na sigurnost tijekom radnog vijeka proizvoda umjetne inteligencije.

Naposljetku, **složeni lanci vrijednosti** utječu na perspektivne digitalne tehnologije. Međutim, ta složenost nije novost ni pitanje poteklo od perspektivnih digitalnih tehnologija kao što su umjetna inteligencija ili internet stvari. To se primjerice odnosi na proizvode kao što su računala, uslužni roboti ili prometni sustavi.

U skladu s okvirom Unije za sigurnost proizvoda, bez obzira na složenost lanca vrijednosti, odgovornost za sigurnost proizvoda ostaje na proizvođaču koji proizvod stavlja na tržište. Proizvođači su odgovorni za sigurnost konačnog proizvoda, uključujući dijelove ugrađene u proizvod, npr. računalni softver.

Neki dijelovi zakonodavstva Unije o sigurnosti proizvoda već sadržavaju odredbe koje se izričito odnose na situacije u kojima nekoliko gospodarskih subjekata djeluje u pogledu određenog proizvoda prije nego što se taj proizvod stavi na tržište. Na primjer, Direktivom o dizalima⁵⁴ zahtijeva se da gospodarski subjekt, koji projektira i proizvodi dizalo, ugraditelju⁵⁵ dostavi „sve potrebne dokumente i podatke” kako bi mu omogućio „točnu i sigurnu ugradnju i ispitivanje dizala”. Direktivom o strojevima zahtijeva se od proizvođača opreme da operateru pruže informacije o načinu sastavljanja te opreme s drugim strojevima⁵⁶.

U zakonodavstvu Unije o sigurnosti proizvoda uzima se u obzir složenost lanaca vrijednosti te se utvrđuju obveze za nekoliko gospodarskih subjekata u skladu s načelom „zajedničke odgovornosti”.

Iako se odgovornost proizvođača za sigurnost konačnog proizvoda pokazala primjerenom za trenutačne složene lance vrijednosti, izričite odredbe kojima se izričito zahtijeva suradnja između gospodarskih subjekata u lancu opskrbe i korisnika mogle bi pružiti pravnu sigurnost u možda još složenijim lancima vrijednosti. Konkretno, svaki sudionik u lancu vrijednosti koji utječe na sigurnost proizvoda (npr. proizvođači softvera) i korisnike (unošenjem izmjene u proizvod) preuzeo bi odgovornost te bi sljedećem sudioniku u lancu pružio potrebne informacije i mjere.

3. Odgovornost

Na razini Unije odredbe o sigurnosti proizvoda i odgovornosti za proizvode dva su komplementarna mehanizma za ostvarivanje istog cilja politike: funkcionalnog jedinstvenog

⁵⁴ U skladu s člankom 16. stavkom 2. Direktive 2014/33/EU.

⁵⁵ U Direktivi 2014/33/EU o dizalima ugraditelj je jednakovrijedan proizvođaču i mora preuzeti odgovornost za projektiranje, proizvodnju, ugradnju i stavljanje dizala na tržište.

⁵⁶ Direktiva o strojevima, članak 1.7.4.2. Priloga I. glasi: „Sve upute za uporabu moraju sadržavati, kada je primjenjivo, najmanje sljedeće podatke:” i „upute za sklapanje, postavljanje i spajanje, uključujući crteže, dijagrame i načine priključivanja i oznaku osovine ili sklopa na koji se stroj postavlja;”

tržišta robe visoke razine sigurnosti, tj. tržišta na kojem se smanjuje rizik od štete za korisnike i osigurava naknada za štetu nastalu zbog neispravne robe.

Na nacionalnoj razini neusklađeni okviri građanskopravne odgovornosti nadopunjuju ta pravila Unije osiguravanjem naknade štete zbog različitih uzroka (kao što su proizvodi i usluge) i uključivanjem različitih odgovornih osoba (kao što su vlasnici, operateri ili pružatelji usluga).

Iako optimizacija sigurnosnih pravila Unije za umjetnu inteligenciju može pomoći u izbjegavanju nesreća, one se ipak mogu dogoditi. U tom slučaju posreduje građanskopravna odgovornost. Pravila o građanskopravnoj odgovornosti imaju dvostruku ulogu u našem društvu: s jedne strane, njima se osigurava da žrtve štete koju su prouzročili drugi dobivaju naknadu, a s druge osiguravaju ekonomske poticaje kako bi odgovorna osoba nastojala izbjeći nastanak takve štete. U propisima o odgovornosti uvijek mora biti uspostavljena ravnoteža između zaštite građana od štete i omogućavanja poduzećima da inoviraju.

Okviri za odgovornost u Uniji dobro su funkcionirali. Temelje se na usporednoj primjeni Direktive o odgovornosti za proizvode (Direktiva 85/374/EEZ), kojom je usklađena odgovornost proizvođača neispravnih proizvoda, i drugih neusklađenih nacionalnih sustava odgovornosti.

Direktivom o odgovornosti za proizvode pruža se razina zaštite koju sama nacionalna subjektivna odgovornost ne pruža. Njome se uvodi sustav objektivne odgovornosti proizvođača za štetu prouzročenu neispravnosću njihovih proizvoda. U slučaju fizičke ili materijalne štete oštećena strana ima pravo na naknadu štete ako dokaže štetu, neispravnost proizvoda (tj. da nije pružio sigurnost koju javnost ima pravo očekivati) i uzročno-posljedičnu vezu između neispravnog proizvoda i štete.

Nacionalni neusklađeni sustavi predviđaju propise koji se temelje na subjektivnoj odgovornosti, u skladu s kojima žrtve štete moraju dokazati krivnju odgovorne osobe, štetu i uzročno-posljedičnu vezu između krivnje i štete kako bi zahtjev za naknadu štete bio uspješan. Njima se predviđaju i sustavi stroge odgovornosti u kojima je nacionalni zakonodavac određenu osobu utvrdio odgovornom za rizik, bez potrebe da žrtva dokaže krivnju/neispravnost ili uzročno-posljedičnu vezu između krivnje/neispravnosti i štete.

Žrtvama štete prouzročene proizvodima i uslugama u nacionalnim je sustavima za odgovornost usporedno na raspolaganju nekoliko mogućih odštetnih zahtjeva koji se temelje na subjektivnoj ili objektivnoj odgovornosti. Ti su zahtjevi često usmjereni protiv različitih odgovornih osoba i imaju različite uvjete.

Na primjer, žrtva koja je sudjelovala u automobilskoj nesreći obično u skladu s nacionalnim građanskim pravom podnosi zahtjev na temelju objektivne odgovornosti protiv vlasnika automobila (tj. osobe koja sklapa ugovor o osiguranju od odgovornosti za upotrebu motornih vozila) i odštetni zahtjev na temelju subjektivne odgovornosti protiv vozača. Usto, u skladu s Direktivom o odgovornosti za proizvode podnosi zahtjev protiv proizvođača u slučaju neispravnosti automobila.

U skladu s usklađenim pravilima o osiguranju motornih vozila, upotreba vozila mora biti osigurana⁵⁷, a osiguravatelj je u praksi uvijek taj kojem se prvo upućuje odštetni zahtjev zbog tjelesne ozljede ili materijalne štete. U skladu s tim pravilima, obveznim osiguranjem žrtvi se

⁵⁷ Usklađeno za motorna vozila Direktivom 2009/103/EZ u odnosu na osiguranje od građanskopravne odgovornosti u pogledu upotrebe motornih vozila i izvršenje obveze osiguranja od takve odgovornosti.

nadoknađuje šteta i štiti osiguranik koji je prema pravilima nacionalnog građanskog prava⁵⁸ dužan platiti novčanu odštetu za nezgodu u kojoj je sudjelovalo motorno vozilo. Proizvođači nisu dužni sklopiti osiguranje na temelju Direktive o odgovornosti za proizvode. Zakonodavstvo Unije ne propisuje nikakvu razliku u obvezi osiguranja neautonomnih i autonomnih vozila. Potonja vozila, kao i sva druga, moraju biti osigurana od odgovornosti za štetu nanesenu trećim osobama, što je najlakši način da oštećena strana dobije naknadu štete.

Sklapanjem odgovarajućeg ugovora o osiguranju mogu se ublažiti posljedice nezgoda tako da se žrtvi neometano isplati naknada štete. Jasna pravila o odgovornosti pomažu osiguravajućim društvima da izračunaju svoje rizike i zatraže povrat od osobe koja je u konačnici odgovorna za štetu. Na primjer, ako je nezgoda uzrokovana neispravnošću, osiguravatelj motornih vozila može zatražiti povrat troškova od proizvođača nakon naknade štete žrtvi.

Karakteristike perspektivnih digitalnih tehnologija kao što su umjetna inteligencija, internet stvari i robotika mogle bi dovesti u pitanje pravne okvire Unije za odgovornost i nacionalne pravne okvire za odgovornost te im smanjiti djelotvornost. Neke od tih karakteristika mogle bi otežati određivanje ljudskog ponašanja kao krivca za štetu, što bi moglo biti temelj za zahtjev na temelju subjektivne odgovornosti u skladu s nacionalnim pravilima. To znači da odštetni zahtjevi koji se temelje na nacionalnim zakonima odgovornosti za štetu mogu biti teški ili preskupi za dokazivanje, zbog čega žrtve možda neće dobiti odgovarajuću naknadu. Važno je da žrtve nezgoda izazvanih proizvodima i uslugama koji uključuju perspektivne digitalne tehnologije kao što je umjetna inteligencija ne budu manje zaštićene u usporedbi sa sličnim drugim proizvodima i uslugama, za koje bi dobili naknadu na temelju nacionalnog zakona o odgovornosti za štetu. U suprotnom bi se društveno prihvaćanje tih tehnologija moglo smanjiti, a oklijevanje pri odlučivanju o njihovoj uporabi povećati.

Bit će potrebno procijeniti bi li izazovi koje nove tehnologije predstavljaju za postojeće okvire mogli uzrokovati pravnu nesigurnost u pogledu načina na koji bi se postojeći zakoni primjenjivali (npr. kako bi se koncept krivnje primjenjivao na štetu prouzročenu umjetnom inteligencijom). To bi zauzvrat moglo obeshrabriti ulaganja i povećati troškove informiranja i osiguranja za proizvođače i druga poduzeća u lancu opskrbe, posebno europska mala i srednja poduzeća. Osim toga, ako se države članice naposljetku uhvate u koštac s izazovima nacionalnih okvira za odgovornost, rascjepkanost bi mogla dodatno porasti, čime bi se povećali troškovi uvođenja inovativnih rješenja umjetne inteligencije i smanjila prekogranična trgovina na jedinstvenom tržištu. Važno je da su poduzeća informirana o rizicima od odgovornosti u cijelom lancu vrijednosti, da ih mogu smanjiti ili spriječiti te se djelotvorno osigurati od njih.

U ovom se poglavlju objašnjava kako nove tehnologije dovode u pitanje postojeće okvire i kako bi se ti izazovi mogli prevladati. Nadalje, za neke bi sektore, na primjer zdravstvenu skrb, zbog njihove specifičnosti mogla biti potrebna dodatna razmatranja.

Složenost proizvoda, usluga i lanca vrijednosti: Tehnologija i industrija drastično su se razvile tijekom posljednjih desetljeća. Konkretno, razgraničenje između proizvoda i usluga možda više nije toliko jasno kao nekad. Proizvodi i pružanje usluga sve su povezani. Iako složeni proizvodi i lanci vrijednosti nisu novi za europsku industriju ni njezin regulatorni model, softver i umjetna inteligencija zaslužuju posebnu pozornost u pogledu odgovornosti za proizvode. Softver je ključan za funkcioniranje velikog broja proizvoda i može utjecati na njihovu sigurnost. Integriran je u proizvode, ali se može isporučiti i odvojeno kako bi se

⁵⁸ U većini je država članica osoba u čije je ime motorno vozilo registrirano objektivno odgovorna.

omogućila predviđena uporaba proizvoda. Ni računalo ni pametni telefon ne bi bili od koristi bez softvera. To znači da softver može opipljiv proizvod učiniti neispravnim i dovesti do fizičkog oštećenja (vidjeti okvir o softveru u dijelu o sigurnosti). To bi u konačnici moglo dovesti do odgovornosti proizvođača proizvoda u skladu s Direktivom o odgovornosti za proizvode.

Međutim, budući da je vrsta i oblika softvera mnogo, nije uvijek jednostavno reći treba li ga razvrstati kao uslugu ili kao proizvod. Stoga, iako bi se softver koji upravlja radom opipljivog proizvoda mogao smatrati njegovim dijelom ili komponentom, neke oblike samostalnog softvera moglo bi biti teže razvrstati.

Iako je definicija proizvoda iz Direktive o odgovornosti za proizvode široka, njezino bi se područje primjene moglo dodatno pojasniti kako bi se bolje odrazila složenost perspektivnih tehnologija i osiguralo da je uvijek dostupna naknada za štetu prouzročenu proizvodima koji su neispravni zbog softvera ili drugih digitalnih značajki. Tako bi gospodarski subjekti, kao što su programeri, mogli procijeniti mogu li se smatrati proizvođačima u skladu s Direktivom o odgovornosti za proizvode.

UI aplikacije često su integrirane u **složena okruženja interneta stvari** u kojima međusobno djeluju mnogi različiti povezani uređaji i usluge. S obzirom na kombinaciju različitih digitalnih komponenti u složenom ekosustavu i mnoštvo uključenih aktera može biti teško procijeniti gdje nastaje potencijalna šteta i koja je osoba za nju odgovorna. Zbog složenosti tih tehnologija žrtvama može biti vrlo teško identificirati odgovornu osobu i dokazati sve potrebne uvjete za uspješan zahtjev, kako je propisano nacionalnim pravom. Troškovi tog stručnog znanja mogu biti previsoki i obeshrabiliti žrtve od traženja naknade.

Osim toga, proizvodi i usluge koji se oslanjaju na umjetnu inteligenciju bit će u interakciji s tradicionalnim tehnologijama, što će povećati složenost i u pogledu odgovornosti. Na primjer, autonomni automobili određeno će vrijeme dijeliti cestu s tradicionalnim automobilima. Slična će se složenost u pogledu sudionika u interakciji pojaviti u nekim uslužnim sektorima (kao što su upravljanje prometom i zdravstvo) u kojima će se djelomično automatiziranim UI sustavima podupirati ljudsko donošenje odluka.

U skladu s Izvješćem⁵⁹ podskupine za nove tehnologije Stručne skupine za odgovornost i nove tehnologije, mogle bi se razmotriti prilagodbe nacionalnih zakona kako bi se žrtvama štete povezane s umjetnom inteligencijom olakšao teret dokazivanja. Na primjer, dokazivati bi možda trebalo je li relevantni operater ispunio posebne obveze u području kibersigurnosti ili druge zakonom utvrđene obveze u pogledu sigurnosti: ako relevantni operater ne poštuje ta pravila, mogao bi snositi teret dokazivanja u pogledu krivnje i uzročnosti.

Komisija prikuplja stajališta o tome treba li i u kojoj mjeri posljedice složenosti ublažiti tako što bi se na razini EU-a predložila inicijativa prema kojoj bi se za štetu prouzročenu primjenom UI aplikacija teret dokazivanja u nacionalnim pravilima olakšao odnosno prenio na drugu stranku.

Kad je riječ o zakonodavstvu Unije, u skladu s Direktivom o odgovornosti za proizvode, proizvod koji ne ispunjava obvezna sigurnosna pravila smatrao bi se neispravnim, bez obzira na krivnju proizvođača. Međutim, mogu postojati i razlozi da se razmotri kako se žrtvama

⁵⁹ *Liability for Artificial Intelligence and other emerging technologies' Report* (Izvješće o odgovornosti za umjetnu inteligenciju i druge perspektivne tehnologije), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

može olakšati teret dokazivanja u skladu s Direktivom: Direktiva se oslanja na nacionalna pravila o dokazivanju i utvrđivanju uzročno-posljedične veze.

Povezivost i otvorenost: Trenutačno nije u potpunosti jasno koja bi mogla biti očekivanja u pogledu štete koja je posljedica povrede kibersigurnosti proizvoda te bi li se takva šteta odgovarajuće nadoknadila u skladu s Direktivom o odgovornosti za proizvode.

Kibersigurnosni nedostaci mogu postojati od samog početka, odnosno stavljanja proizvoda na tržište, ali se mogu pojaviti i znatno kasnije.

U okvirima koji se temelje na subjektivnoj odgovornosti, uspostavom jasnih obveza u području kibersigurnosti operaterima se omogućuje da utvrde što moraju učiniti kako bi izbjegli posljedice odgovornosti.

U skladu s Direktivom o odgovornosti za proizvode, pitanje je li proizvođač mogao predvidjeti određene promjene uzimajući u obzir razumno predvidivu uporabu proizvoda može dobiti na važnosti. Na primjer, može se primijetiti povećanje uporabe „obrane kasnijom neispravnosću” prema kojoj proizvođač nije odgovoran ako proizvod nije bio neispravan u trenutku stavljanja na tržište ili „obrane rizikom naknadnog razvoja” (da se uz najnovije spoznaje u tom trenutku neispravnost nije mogla predvidjeti). Osim toga, odgovornost bi se mogla smanjiti ako oštećena strana ne izvršava relevantna sigurnosna ažuriranja. To bi se potencijalno moglo smatrati postupkom oštećene osobe koji je pridonio šteti, čime bi se smanjila odgovornost proizvođača. Budući da bi pojam razumno predvidive uporabe i pitanja u pogledu postupka oštećene osobe koji je pridonio šteti, primjerice nepreuzimanja sigurnosnog ažuriranja, mogli imati veću važnost, oštećenim bi osobama moglo biti teže dobiti naknadu za štetu prouzročenu neispravnosću proizvoda.

Autonomija i netransparentnost: Ako UI aplikacije mogu djelovati autonomno, za njih se ne moraju unaprijed definirati svi koraci za obavljanje zadaće, a neposredna ljudska kontrola ili nadzor može dijelom ili u cijelosti izostati. Algoritme koji se temelje na strojnom učenju može biti teško, ako ne i nemoguće, razumjeti (učinak crne kutije).

Osim prethodno navedene složenosti, učinak crne kutije u nekim bi sustavima umjetne inteligencije mogao biti takav da otežava dobivanje naknade za štetu prouzročenu autonomnim aplikacijama takvih sustava. Da bi algoritme i podatke koje umjetna inteligencija upotrebljava bilo moguće razumjeti, potrebni su analitički kapacitet i tehničko stručno znanje, a oni bi žrtvama mogli biti preskupi. Osim toga, pristup algoritmu i podacima mogao bi biti nemoguć bez suradnje potencijalno odgovorne osobe. Žrtve stoga u praksi možda neće moći podnijeti odštetni zahtjev. Uz to, bilo bi nejasno kako dokazati krivnju autonomnog djelovanja umjetne inteligencije ili što bi se smatralo krivnjom osobe koja se oslonila na upotrebu umjetne inteligencije.

U nacionalnim zakonima već je izrađen niz rješenja da se žrtvama olakša teret dokazivanja u sličnim situacijama.

Vodeće načelo za sigurnost proizvoda i odgovornost za proizvode u Uniji ostaje da su proizvođači odgovorni za to da svi proizvodi stavljeni na tržište budu sigurni tijekom njihova životnog ciklusa i za uporabu koja se razumno može očekivati. To znači da bi proizvođač morao osigurati da proizvod koji koristi umjetnu inteligenciju poštuje određene sigurnosne parametre. Značajke umjetne inteligencije ne isključuju pravo na očekivanja u pogledu sigurnosti proizvoda, neovisno o tome je li riječ o automatskim kosilicama trave ili kirurškim robotskim sustavima.

Autonomija može utjecati na sigurnost proizvoda jer može znatno izmijeniti njegove karakteristike, uključujući sigurnosne. Pitanje je pod kojim uvjetima samostalno učenje ima

za posljedicu produljenje odgovornosti proizvođača i u kojoj je mjeri proizvođač trebao predvidjeti određene promjene.

Pojam „stavljanje na tržište” koji se trenutačno upotrebljava u Direktivi o odgovornosti za proizvode mogao bi se, vodeći računa o usklađenosti s odgovarajućim promjenama okvira Unije za sigurnost, preispitati kako bi se uzelo u obzir da se proizvodi mogu mijenjati sami i da ih se može izmijeniti. To bi moglo pomoći i u tome da se razjasni tko je odgovoran za promjene proizvoda.

Prema Izvješću⁶⁰ podskupine za nove tehnologije Stručne skupine za odgovornost i nove tehnologije, rad nekih autonomnih uređaja i usluga umjetne inteligencije mogao bi imati poseban profil u pogledu rizika u smislu odgovornosti jer može uzrokovati znatnu štetu važnim pravnim interesima kao što su život, zdravlje i imovina te izložiti širu javnost rizicima. To bi se moglo uglavnom odnositi na uređaje umjetne inteligencije koji se kreću u javnim prostorima (npr. potpuno autonomna vozila, bespilotne letjelice⁶¹ i roboti za dostavu paketa) ili usluge koje se temelje na umjetnoj inteligenciji sa sličnim rizicima (npr. usluge upravljanja prometom koje usmjeravaju ili kontroliraju vozila ili usluga upravljanja distribucijom električne energije). Izazovi u pogledu autonomije i netransparentnosti nacionalnih zakona o odgovornosti za štetu mogli bi se prevladati pristupom koji se temelji na riziku. Sustavi objektivne odgovornosti mogli bi osigurati da žrtva dobije naknadu neovisno o krivnji kad god se taj rizik ostvari. Trebalo bi pažljivo procijeniti učinak koji odabir objektivno odgovornih osoba za takve operacije ima na razvoj i primjenu umjetne inteligencije te razmotriti pristup utemeljen na riziku.

Kad je riječ o funkcioniranju UI aplikacija s posebnim profilom u pogledu rizika, Komisija traži mišljenja o tome je li i u kojoj mjeri nužna objektivna odgovornost, kako postoji u nacionalnim zakonima za slične rizike kojima je izložena javnost (na primjer za upravljanje motornim vozilima, zrakoplovima ili nuklearnim elektranama), da bi se mogućim žrtvama šteta učinkovito nadoknađivala. Komisija traži i mišljenja o povezivanju objektivne odgovornosti s mogućom obvezom sklapanja ugovora o dostupnom osiguranju, slijedeći primjer Direktive o osiguranju motornih vozila, kako bi se naknada štete osigurala neovisno o solventnosti odgovorne osobe, a troškovi štete smanjili.

Za funkcioniranje svih drugih, odnosno velike većine UI aplikacija, Komisija razmatra treba li prilagoditi teret dokazivanja uzročno-posljedične veze i krivnje. U tom pogledu, jedno od pitanja istaknutih u Izvješću⁶² podskupine za nove tehnologije Stručne skupine za odgovornost i nove tehnologije jest situacija u kojoj potencijalno odgovorna osoba nije zabilježila podatke relevantne za procjenu odgovornosti ili ih nije voljna podijeliti sa žrtvom.

⁶⁰ *Liability for Artificial Intelligence and other emerging technologies' Report* (Izvješće o odgovornosti za umjetnu inteligenciju i druge perspektivne tehnologije), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

⁶¹ Vidjeti sustave bespilotnih zrakoplova iz Provedbene uredbe Komisije (EU) 2019/947 od 24. svibnja 2019. o pravilima i postupcima za rad bespilotnih zrakoplova.

⁶² *Liability for Artificial Intelligence and other emerging technologies' Report* (Izvješće o odgovornosti za umjetnu inteligenciju i druge perspektivne tehnologije), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

4. Zaključak

Pojava novih digitalnih tehnologija kao što su umjetna inteligencija, internet stvari i robotika donosi nove izazove u pogledu sigurnosti proizvoda i odgovornosti kao što su povezivost, autonomija, ovisnost o podacima, netransparentnost, složenost proizvoda i sustava, ažuriranja softvera, složenije upravljanje sigurnošću i složeniji lanci vrijednosti.

Postojeće zakonodavstvo o sigurnosti proizvoda sadržava niz nedostataka koje je potrebno ukloniti, posebno u Direktivi o općoj sigurnosti proizvoda, Direktivi o strojevima, Direktivi o radijskoj opremi i novom zakonodavnom okviru. Budući rad na prilagodbi različitih zakonodavnih akata u tom okviru obavljat će se na dosljedan i usklađen način.

Novi izazovi u pogledu sigurnosti stvaraju i nove izazove u pogledu odgovornosti. S tim se izazovima povezanim s odgovornošću treba uhvatiti u koštac kako bi zaštita bila jednaka kao za žrtve tradicionalnih tehnologija, uz istodobno održavanje ravnoteže s potrebama tehnoloških inovacija. To će pomoći u stvaranju povjerenja u te perspektivne digitalne tehnologije i omogućiti stabilnost ulaganja.

Iako postojeći propisi Unije i nacionalni zakoni o odgovornosti u načelu sadržavaju odredbe koje se mogu odnositi na poteškoće koje donose perspektivne tehnologije, veličina i kombinirani učinak izazova umjetne inteligencije mogli bi otežati isplatu naknade žrtvama u slučajevima u kojima bi to bilo opravdano⁶³. Stoga raspodjela troškova u slučaju nastanka štete može biti nepoštena ili neučinkovita prema trenutačnim pravilima. Kako bi se to ispravilo i kako bi se pojasnile moguće nesigurnosti u postojećem okviru, na razini EU-a mogle bi se pokrenuti inicijative kako bi se na temelju ciljanog pristupa temeljenog na riziku, tj. uzimajući u obzir da različite UI aplikacije predstavljaju različite rizike, razmotrile određene prilagodbe Direktive o odgovornosti za proizvode i nacionalnih sustava odgovornosti.

⁶³ Vidjeti Izvješće podskupine za nove tehnologije, str. 3. i preporuku politike 27.2. Stručne skupine na visokoj razini o umjetnoj inteligenciji.