EVROPSKA
KOMISIJA

Bruselj, 19.2.2020
COM(2020) 64 final

POROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU IN EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU

Poročilo o vprašanjih varnosti in odgovornosti, ki jih sprožajo umetna inteligenca, internet stvari in robotika

POROČILO O VPRAŠANJIH VARNOSTI IN ODGOVORNOSTI, KI JIH SPROŽAJO UMETNA INTELIGENCA, INTERNET STVARI IN ROBOTIKA

1. Uvod

Umetna inteligenca[1], internet stvari[2] in robotika bodo ustvarili nove priložnosti in koristi za našo družbo. Komisija je prepoznala pomen in potencial teh tehnologij, pa tudi potrebo po znatnih naložbah na teh področjih[3]. Zavezana je cilju, da Evropa postane vodilna v svetu na področjih umetne inteligence, interneta stvari in robotike. Za dosego tega cilja je potreben jasen in predvidljiv pravni okvir, ki bo obravnaval tehnološke izzive.

1.1. Obstoječi okvir za varnost in odgovornost

Splošni cilj pravnih okvirov za varnost in odgovornost je zagotoviti, da vsi proizvodi in storitve, vključno s tistimi z integriranimi digitalnimi tehnologijami v vzponu, delujejo varno, zanesljivo in dosledno ter da se morebitna nastala škoda učinkovito odpravi. Visoka raven varnosti proizvodov in sistemov z integriranimi novimi digitalnimi tehnologijami ter trdni mehanizmi za odpravljanje nastale škode (tj. okvir za odgovornost) prispevajo k boljšemu varstvu potrošnikov. Prav tako ustvarjajo zaupanje v te tehnologije, kar je predpogoj za njihovo sprejemanje v industriji in pri uporabnikih. To bo posledično spodbudilo konkurenčnost naše industrije in prispevalo k uresničevanju ciljev Unije[4]. Jasen okvir za varnost in odgovornost je še posebej pomemben, ko se pojavijo nove tehnologije, kot so umetna inteligenca, internet stvari in robotika, in sicer zato, da se zagotovita varstvo potrošnikov in pravna varnost podjetij.

Unija ima robusten in zanesljiv regulativni okvir na področju varnosti in odgovornosti za proizvode ter trden sklop varnostnih standardov, ki jih dopolnjujejo nacionalne, neharmonizirane zakonodaje o odgovornosti. Skupaj zagotavljajo blaginjo naših državljanov na enotnem trgu ter spodbujajo inovacije in uvajanje novih tehnologij. Vendar pa umetna inteligenca, internet stvari in robotika spreminjajo značilnosti številnih proizvodov in storitev.

V sporočilu o umetni inteligenci za Evropo[5], sprejetem 25. aprila 2018, je bilo napovedano, da bo Komisija predložila poročilo z oceno posledic digitalnih tehnologij v vzponu za obstoječa okvira varnosti in odgovornosti. Namen tega poročila je opredeliti in preučiti širše posledice in morebitne vrzeli v okvirih odgovornosti in varnosti za umetno inteligenco, internet stvari in robotiko. Smernice iz tega poročila, ki spremlja belo knjigo o umetni inteligenci, so predvidene za razpravo in so del širšega posvetovanja z deležniki. Oddelek o varnosti temelji na oceni[6] direktive o strojih[7] in delu z zadevnimi strokovnimi skupinami[8].

---

[1] Opredelitev umetne inteligence, kot jo je sprejela strokovna skupina na visoki ravni za umetno inteligenco, je na voljo na https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines.

[2] Opredelitev interneta stvari iz Priporočila ITU-T Y.2060 je na voljo na https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

[3] SWD(2016) 110, COM(2017) 9, COM(2018) 237 in COM(2018) 795.

[4] http://ec.europa.eu/growth/industry/policy_sl.

[5] https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=COM%3A2018%3A237%3AFIN.
V spremnem delovnem dokumentu služb Komisije (2018) 137 (https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137) so prvič opisani izzivi na področju odgovornosti, ki se pojavljajo v kontekstu digitalnih tehnologij v vzponu.

[6] SWD(2018) 161 final.

Oddelek o odgovornosti temelji na oceni[9] direktive o odgovornosti za proizvode[10], prispevkih zadevnih strokovnih skupin[11] in stikih z deležniki. Namen tega poročila ni, da se zagotovi izčrpen pregled obstoječih pravil o varnosti in odgovornosti, temveč da se pozornost nameni ključnim doslej opredeljenim vprašanjem.

1.2. Značilnosti tehnologij umetne inteligence, interneta stvari in robotike

Umetna inteligenca, internet stvari in robotika imajo veliko skupnih značilnosti. Z združevanjem **povezljivosti**, **avtonomnosti** in **podatkovne odvisnosti** lahko izvajajo naloge z malo ali nič človeškega nadzora. Sistemi, ki so opremljeni z umetno inteligenco, lahko izboljšajo svojo zmogljivost z učenjem iz izkušenj. Njihova **kompleksnost** se odraža v množici gospodarskih subjektov, vključenih v **dobavno verigo**, in raznovrstnosti sestavnih delov, elementov, programske opreme, sistemov ali storitev, ki skupaj tvorijo nove tehnološke ekosisteme. Poleg tega so po tem, ko so dani na trg, **odprti** za posodobitve in nadgradnje. Velike količine podatkov, zanašanje na algoritme in **nepreglednost** postopka odločanja umetne inteligence otežujejo napovedovanje vedenja proizvodov, podprtih z umetno inteligenco, in razumevanje možnih vzrokov za škodo. Povezljivost in odprtost pa lahko tudi povzročita, da so proizvodi, ki temeljijo na umetni inteligenci in internetu stvari, izpostavljeni **kibernetskim grožnjam**.

1.3. Priložnosti, ki jih ustvarjajo umetna inteligenca, internet stvari in robotika

Povečanje zaupanja uporabnikov in družbenega sprejemanja tehnologij v vzponu, izboljšanje proizvodov, postopkov in poslovnih modelov ter pomoč evropskim proizvajalcem, da postanejo učinkovitejši, so le nekatere priložnosti, ki jih ponujajo umetna inteligenca, internet stvari in robotika.

Poleg izboljšanja produktivnosti in učinkovitosti naj bi umetna inteligenca ljudem omogočila razvoj še ne dosežene inteligence, odprla vrata novim odkritjem in pomagala pri reševanju nekaterih največjih svetovnih izzivov: od zdravljenja kroničnih bolezni, napovedovanja izbruhov bolezni ali zmanjšanja števila smrtnih žrtev v prometnih nesrečah do boja proti podnebnim spremembam ali predvidevanja kibernetskih groženj.

Te tehnologije lahko z izboljšanjem varnosti proizvodov prinesejo številne koristi, saj bodo ti manj izpostavljeni določenim tveganjem. Povezana in avtomatizirana vozila bi lahko na primer izboljšala varnost v cestnem prometu, saj je večina prometnih nesreč trenutno

---

7 Direktiva 2006/42/ES.

8 Mreža za varnost potrošnikov, kot je določena v Direktivi 2001/95/ES o splošni varnosti proizvodov, ter strokovni skupini za Direktivo 2006/42/ES o strojih in Direktivo 2014/53/EU o radijski opremi, v katerih sodelujejo države članice, industrija in drugi deležniki, kot so združenja potrošnikov.

9 COM(2018) 246 final.

10 Direktiva 85/374/EGS.

11 Strokovna skupina za odgovornost in nove tehnologije je bila ustanovljena, da bi Komisiji zagotovila strokovno znanje o uporabnosti direktive o odgovornosti za proizvode in nacionalnih predpisov o civilni odgovornosti ter pomoč pri razvoju vodilnih načel za morebitne prilagoditve veljavnih zakonov, povezanih z novimi tehnologijami. Sestavljena je iz dveh podskupin, in sicer „podskupine za odgovornost za proizvode“ in „podskupine za nove tehnologije“, glej http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1.
Za poročilo „podskupine za nove tehnologije“ o odgovornosti za umetno inteligenco in druge tehnologije v vzponu glej https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

posledica človeških napak[12]. Poleg tega so sistemi interneta stvari zasnovani za sprejemanje in obdelavo velikih količin podatkov iz različnih virov. To veliko količino informacij bi lahko izkoristili, da bi se proizvodi sami prilagajali in s tem postali varnejši. Nove tehnologije lahko prispevajo k učinkovitejšemu odpoklicu proizvodov, saj bi lahko na primer proizvodi sami opozarjali uporabnike na varnostne težave[13]. Če se med uporabo povezanega proizvoda pojavi varnostno vprašanje, lahko proizvajalci neposredno stopijo v stik z uporabniki, da jih opozorijo na tveganja in, če je to mogoče, takoj odpravijo težavo, na primer z varnostno posodobitvijo. Tako je na primer proizvajalec pametnega telefona leta 2017 med odpoklicem ene od svojih naprav izvedel posodobitev programske opreme, da bi zmogljivost baterije v odpoklicanih telefonih zmanjšal na 0 %[14], tako da bi uporabniki prenehali uporabljati nevarne naprave.

Poleg tega lahko nove tehnologije prispevajo k boljši sledljivosti proizvodov. Funkcije povezljivosti interneta stvari lahko na primer podjetjem in organom za nadzor trga omogočijo, da spremljajo nevarne proizvode in ugotovijo tveganja v dobavnih verigah[15].

Poleg tega, da umetna inteligenca, internet stvari in robotika prinašajo priložnosti za gospodarstvo in naše družbe, pa lahko tudi ogrozijo pravno zaščitene interese, tako materialne kot nematerialne. Tveganje za take grožnje se bo povečalo s širjenjem uporabe teh tehnologij. V zvezi s tem je treba analizirati, ali in v kolikšni meri je sedanji pravni okvir varnosti in odgovornosti še vedno primeren za zaščito uporabnikov.

2. Varnost

V sporočilu Komisije o krepitvi zaupanja v umetno inteligenco, osredotočeno na človeka, je navedeno, da ***morajo imeti sistemi umetne inteligence zaščitne in vgrajene varnostne mehanizme, ki zagotavljajo, da so sistemi preverljivo varni na vsakem koraku****, pri čemer mora biti glavna skrb* ***fizična in psihična varnost*** *vseh zadevnih oseb*[16].

Pri oceni zakonodaje Unije o varnosti proizvodov v tem oddelku je analizirano, ali sedanji zakonodajni okvir Unije vsebuje ustrezne elemente za zagotovitev, da imajo tehnologije v vzponu in zlasti sistemi umetne inteligence vgrajene zaščitne in varnostne mehanizme.

To poročilo obravnava predvsem direktivo o splošni varnosti proizvodov[17] in harmonizirano zakonodajo o proizvodih, ki upošteva horizontalna pravila „novega pristopa“[18] in/ali „novega

---

[12] Po ocenah so za približno 90 % prometnih nesreč krive človeške napake. Glej poročilo Komisije „Reševanje življenj: spodbujanje varnosti vozil v EU“ (COM(2016) 787 final).

[13] Voznika avtomobila je na primer mogoče opozoriti, naj upočasni, če se je na cesti, po kateri vozi, zgodila nesreča.

[14] OECD (2018), „Measuring and maximising the impact of product recalls globally: OECD workshop report“ (Merjenje in povečevanje učinka odpoklica proizvodov po svetu: poročilo delavnice OECD), *OECD Science, Technology and Industry Policy Papers*, št. 56, OECD Publishing, Pariz, https://doi.org/10.1787/ab757416-en.

[15] OECD (2018), „Enhancing product recall effectiveness globally: OECD background report“ (Povečanje učinkovitosti odpoklica proizvodov po svetu: osnovno poročilo OECD), *OECD Science, Technology and Industry Policy Papers*, št. 58, OECD Publishing, Pariz, https://doi.org/10.1787/ef71935c-en.

[16] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o krepitvi zaupanja v umetno inteligenco, osredotočeno na človeka, Bruselj, 8.4.2019, COM(2019) 168 final.

[17] Direktiva 2001/95/ES Evropskega parlamenta in Sveta z dne 3. decembra 2001 o splošni varnosti proizvodov (UL L 11, 15.1.2002, str. 4).

[18] UL C 136, 4.6.1985, str. 1.

zakonodajnega okvira“ (v nadaljnjem besedilu: zakonodaja ali okvir Unije za varnost proizvodov)[19]. Horizontalna pravila zagotavljajo skladnost med sektorskimi pravili o varnosti proizvodov.

Namen zakonodaje Unije o varnosti proizvodov je zagotoviti, da proizvodi, dani na trg Unije, izpolnjujejo visoke zdravstvene, varnostne in okoljske zahteve ter da lahko taki proizvodi prosto krožijo po vsej Uniji. Sektorsko zakonodajo[20] dopolnjuje direktiva o splošni varnosti proizvodov[21], ki zahteva, da morajo biti varni vsi potrošniški proizvodi, tudi če jih ne ureja sektorska zakonodaja EU. Varnostne predpise dopolnjujejo mehanizmi za nadzor trga in pooblastila, ki jih imajo nacionalni organi na podlagi uredbe o nadzoru trga[22] in direktive o splošni varnosti proizvodov[23]. Na področju prometa obstajajo dodatna pravila Unije in nacionalna pravila za začetek obratovanja motornih vozil[24], zrakoplovov ali ladij ter jasna pravila, ki urejajo varnost med obratovanjem, vključno z nalogami za upravljavce in nalogami nadzora, ki jih opravljajo organi.

Evropska standardizacija je prav tako bistven element zakonodaje Unije o varnosti proizvodov. Glede na globalno naravo digitalizacije in digitalnih tehnologij v vzponu je mednarodno sodelovanje pri standardizaciji posebej pomembno za konkurenčnost evropske industrije.

Velik del okvira Unije za varnost proizvodov je bil napisan pred pojavom digitalnih tehnologij, kot so umetna inteligenca, internet stvari ali robotika. Zato ne vsebuje določb, ki bi izrecno obravnavale nove izzive in tveganja v povezavi s temi novimi tehnologijami. Ker pa je obstoječi okvir za varnost proizvodov tehnološko nevtralen, to ne pomeni, da se ne uporablja za proizvode, ki vključujejo te tehnologije. Poleg tega poznejši zakonodajni akti, ki so del navedenega okvira, na primer o medicinskih pripomočkih ali avtomobilih, že izrecno obravnavajo nekatere vidike pojavljanja digitalnih tehnologij, npr. avtomatizirane odločitve, programsko opremo kot ločen proizvod in povezljivost.

[19] Uredba (ES) št. 2008/765 in Odločba (ES) št. 2008/768.

[20] Ta shema ne vključuje zakonodaje Unije o prevozu in avtomobilih.

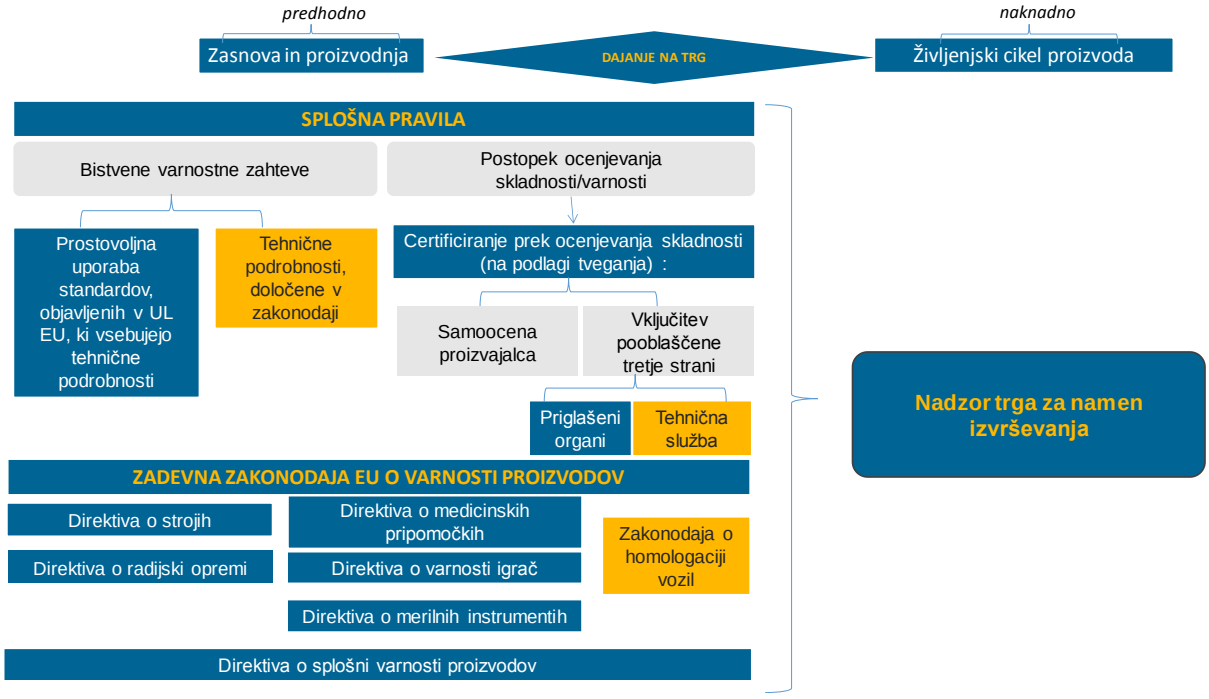
[21] Direktiva 2001/95/ES Evropskega parlamenta in Sveta z dne 3. decembra 2001 o splošni varnosti proizvodov (UL L 11, 15.1.2002, str. 4).

[22] Uredba (ES) št. 765/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o določitvi zahtev za akreditacijo in nadzor trga v zvezi s trženjem proizvodov ter razveljavitvi Uredbe (EGS) št. 339/93 (UL L 218, 13.8.2008, str. 30), ELI: https://eur-lex.europa.eu/eli/reg/2008/765/oj?locale=sl, in, od leta 2021 naprej, Uredba (EU) 2019/1020 Evropskega parlamenta in Sveta z dne 20. junija 2019 o nadzoru trga in skladnosti proizvodov ter spremembi Direktive 2004/42/ES in uredb (ES) št. 765/2008 in (EU) št. 305/2011, UL L 169, 25.6.2019, str. 1, ELI: https://eur-lex.europa.eu/eli/reg/2019/1020/oj?locale=sl.

[23] Člen 8(1)(b) in (3) direktive o splošni varnosti proizvodov.

[24] Na primer Direktiva 2007/46/ES o odobritvi motornih in priklopnih vozil ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila, in Uredba (EU) 2018/858 Evropskega parlamenta in Sveta z dne 30. maja 2018 o odobritvi in tržnem nadzoru motornih vozil in njihovih priklopnikov ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila, spremembi uredb (ES) št. 715/2007 in (ES) št. 595/2009 ter razveljavitvi Direktive 2007/46/ES.

Osnovna logika veljavne zakonodaje Unije o varnosti proizvodov[25]



Izzivi, ki jih v okvir Unije za varnost proizvodov prinašajo digitalne tehnologije v vzponu, so predstavljeni v nadaljevanju.

Povezljivost je osrednji element vedno večjega števila proizvodov in storitev. Ta značilnost na preizkušnjo postavlja tradicionalni koncept varnosti, saj lahko povezljivost varnost proizvoda ogrozi neposredno ali pa posredno, kadar je mogoče vanj vdreti, kar vodi do varnostnih groženj in vpliva na varnost uporabnikov.

Primer tega je naveden v obvestilu Islandije, poslanem po sistemu hitrega obveščanja EU, ki se nanaša na pametno zapestno uro za otroke[26]. Ta proizvod ne bi povzročil neposredne škode za otroka, ki ga nosi, toda ker ni zagotovljena minimalna raven varnosti, ga je mogoče z lahkoto uporabiti kot orodje za dostop do otroka. Ker je ena od predvidenih funkcij proizvoda varovanje otrok z lokalizacijo, bi potrošnik pričakoval, da ne predstavlja tveganj za otroke, ki bi lahko vplivala na njihovo varnost, na primer tako, da bi jih lahko kdor koli izsledil in/ali z njimi stopil v stik.

Drug primer je naveden v obvestilu, ki ga je predložila Nemčija v zvezi z osebnimi avtomobili[27]. Radijski sprejemnik v avtomobilu ima lahko določene vrzeli glede varnosti programske opreme, ki nepooblaščenim tretjim osebam omogočajo dostop do medsebojno povezanih krmilnih sistemov v vozilu. Če bi tretje osebe te vrzeli v varnosti programske opreme izkoristile za zlonamerne namene, bi lahko prišlo do prometne nesreče.

Če industrijske aplikacije nimajo potrebne ravni zaščite, so lahko izpostavljene kibernetskim grožnjam, ki vplivajo na varnost ljudi v večjem obsegu. To lahko velja na primer za kibernetske napade na kritični nadzorni sistem industrijskega obrata, ki bi lahko sprožili eksplozijo, pri kateri bi prišlo do smrtnih žrtev.

---

[25] Ta slika ne vključuje zahtev zakonodaje o življenjskem ciklu proizvodov, tj. uporabe in vzdrževanja, in je predstavljena samo za splošno ponazoritev.

[26] Obvestilo RAPEX Islandije, objavljeno na spletišču EU Safety Gate (A12/0157/19).

[27] Obvestilo RAPEX Nemčije, objavljeno na spletišču EU Safety Gate (A12/1671/15).

Zakonodaja Unije o varnosti proizvodov na splošno ne določa posebnih obveznih bistvenih zahtev za preprečevanje kibernetskih groženj, ki bi vplivale na varnost uporabnikov. Vendar pa v uredbi o medicinskih pripomočkih[28], direktivi o merilnih instrumentih[29], direktivi o radijski opremi[30] ali zakonodaji o homologaciji vozil[31] obstajajo določbe v zvezi z varnostnimi vidiki. Akt o kibernetski varnosti[32] vzpostavlja prostovoljni okvir certificiranja za proizvode, storitve in postopke informacijske in komunikacijske tehnologije na področju kibernetske varnosti, ustrezna zakonodaja Unije o varnosti proizvodov pa določa obvezne zahteve.

Poleg tega lahko tveganje izgube povezljivosti pri digitalnih tehnologijah v vzponu pomeni tudi varnostna tveganja. Če na primer povezani požarni alarm izgubi povezljivost, se lahko zgodi, da uporabnika ne bo opozoril v primeru požara.

V sedanji zakonodaji Unije o varnosti proizvodov je varnost cilj javne politike. Koncept varnosti je povezan z uporabo proizvoda in tveganji, npr. mehanskimi, električnimi itd., ki jih je treba obravnavati, da se zagotovi varnost proizvoda. Opozoriti je treba, da v različnih aktih Unije o varnosti proizvodov uporaba proizvoda zajema tako predvideno kot predvidljivo uporabo, v nekaterih primerih, na primer v direktivi o strojih[33], pa tudi razumno predvidljivo napačno uporabo.

Koncept varnost v veljavni zakonodaji Unije o varnosti proizvodov je v skladu z razširjenim konceptom varnosti za zaščito potrošnikov in uporabnikov. Koncept varnosti proizvodov tako zajema zaščito pred vsemi vrstami tveganj, ki izhajajo iz proizvoda, kar vključuje ne le mehanska, kemična in električna tveganja, temveč tudi kibernetska tveganja in tveganja, povezana z izgubo povezljivosti naprav.

V zvezi s tem bi lahko razmislili o izrecnih določbah za področja uporabe zadevnih zakonodajnih aktov Unije, da bi zagotovili boljšo zaščito uporabnikov in večjo pravno varnost.

Avtonomnost[34] je ena od glavnih značilnosti umetne inteligence. Neželene posledice uporabe umetne inteligence bi lahko škodovale uporabnikom in izpostavljenim osebam.

Za primere, ko je prihodnje „vedenje“ proizvodov umetne inteligence mogoče vnaprej določiti z oceno tveganja, ki jo proizvajalec izvede pred dajanjem proizvodov na trg, okvir Unije za varnost proizvodov že določa obveznosti za proizvajalce, da v oceni tveganja upoštevajo „uporabo“[35] proizvodov skozi vso življenjsko dobo. Predvideva tudi, da morajo proizvajalci zagotoviti navodila in varnostne informacije za uporabnike ali opozorila[36]. V tem

[28] Uredba (EU) 2017/745 o medicinskih pripomočkih.
[29] Direktiva 2014/32/EU o dostopnosti merilnih instrumentov na trgu.
[30] Direktiva 2014/53/EU o radijski opremi.
[31] Direktiva 2007/46/ES o odobritvi motornih in priklopnih vozil ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila. Direktivo bo 1. septembra 2020 razveljavila in nadomestila Uredba (EU) 2018/858 o odobritvi motornih vozil in njihovih priklopnikov ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila, spremembi uredb (ES) št. 715/2007 in (ES) št. 595/2009 ter razveljavitvi Direktive 2007/46/ES.
[32] Uredba (EU) 2019/881.
[33] Direktiva 2006/42/ES o strojih.
[34] Proizvodi, ki temeljijo na umetni inteligenci, lahko z dojemanjem svojega okolja delujejo avtonomno, ne da bi upoštevali niz vnaprej določenih navodil, vendar njihovo obnašanje omejujejo cilj, ki jim je bil določen, in druge ustrezne konstrukcijske odločitve, ki so jih sprejeli razvijalci teh proizvodov.
[35] Po zakonodaji Unije o varnosti proizvodov proizvajalci opravijo oceno tveganja na podlagi predvidene uporabe proizvoda, predvidljive uporabe in/ali razumno predvidljive napačne uporabe.
[36] Sklep št. 768/2008/ES Evropskega parlamenta in Sveta z dne 9. julija 2008 o skupnem okviru za trženje proizvodov in razveljavitvi Sklepa Sveta 93/465/EGS (UL L 218, 13.8.2008, str. 82). Člen R2.7 Priloge I

smislu Direktiva o radijski opremi[37] na primer zahteva, da proizvajalec v navodila vključi informacije o tem, kako uporabljati radijsko opremo v skladu z njeno predvideno uporabo.

V prihodnosti lahko pride tudi do primerov, ko posledic uporabe sistemov umetne inteligence ne bo mogoče v celoti določiti vnaprej. V takih primerih ocena tveganja, opravljena pred dajanjem proizvoda na trg, morda ne bo več odražala uporabe, delovanja ali vedenja proizvodov. Če se uporaba, ki jo je prvotno predvidel proizvajalec, spremeni[38] zaradi avtonomnega vedenja proizvoda in če to vpliva na skladnost z varnostnimi zahtevami, se lahko razmisli o zahtevi, da se opravi ponovna ocena proizvoda, zmožnega samoučenja[39].

V sedanjem okviru se od proizvajalcev že zahteva, da takoj, ko ugotovijo, da proizvod v svojem življenjskem ciklu predstavlja tveganja, ki vplivajo na varnost, obvestijo pristojne organe in sprejmejo ukrepe za preprečevanje ogrožanja uporabnikov[40].

Poleg ocene tveganja, ki je bila opravljena pred dajanjem proizvoda na trg, bi lahko uvedli nov postopek za oceno tveganja, če pri proizvodu v času njegove življenjske dobe pride do bistvenih sprememb, npr. dobi drugo funkcijo, ki jo proizvajalec ni predvidel v prvotni oceni tveganja. Ta postopek bi se morali osredotočiti na vpliv na varnost, ki ga ima avtonomno vedenje proizvoda v celotni življenjski dobi. Oceno tveganja bi moral izvesti ustrezen gospodarski subjekt. Poleg tega bi lahko ustrezni zakonodajni akti Unije vključevali okrepljene zahteve za proizvajalce v zvezi z navodili in opozorili za uporabnike.

Podobne ocene tveganja se že zahtevajo v zakonodaji na področju prometa[41]; na primer, zakonodaja o železniškem prometu zahteva, da v primeru, ko se železniško vozilo spremeni po izdaji spričevala, avtor spremembe izvede poseben postopek, prav tako pa vsebuje jasna merila za določitev, ali je treba vključiti tudi ustrezni organ.

Funkcija samoučenja proizvodov in sistemov umetne inteligence lahko omogoči, da naprava sprejema odločitve, ki odstopajo od tega, kar je prvotno predvidel proizvajalec, in posledično od tega, kar pričakujejo uporabniki. To sproža vprašanja o človeškem nadzoru, saj bi morali ljudje imeti možnost, da izberejo, kako, če sploh, bodo odločitve prepustili proizvodom in

---

določa: „*Proizvajalci zagotovijo, da so proizvodu priložena navodila in varnostne informacije v jeziku, ki ga potrošniki in drugi končni uporabniki brez težav razumejo, kot ga določi zadevna država članica*“.

37 Člen 10(8), ki se nanaša na navodila za končne uporabnike, in Priloga VI, ki se nanaša na izjavo EU o skladnosti.

38 Za zdaj se pojem „samoučenje“ v kontekstu umetne inteligence uporablja predvsem za ponazoritev, da so se naprave med usposabljanjem sposobne učiti; zaenkrat se od naprav, ki temeljijo na umetni inteligenci, ne zahteva, da se učijo tudi po tem, ko se začnejo uporabljati; nasprotno, zlasti v zdravstvu se naprave z umetno inteligenco po uspešno končanem usposabljanju običajno prenehajo učiti. Zato na tej stopnji avtonomno obnašanje, ki izhaja iz sistemov umetne inteligence, ne pomeni, da proizvod opravlja naloge, ki jih razvijalci niso predvideli.

39 To je v skladu z oddelkom 2.1 „Modrega vodnika“ za izvajanje predpisov EU o proizvodih 2016.

40 Člen 5 Direktive 2001/95/ES Evropskega parlamenta in Sveta z dne 3. decembra 2001 o splošni varnosti proizvodov.

41 V primeru kakršne koli spremembe železniškega sistema, ki bi lahko vplivala na varnost (npr. tehnične, operativne spremembe ali organizacijske spremembe, ki bi lahko vplivale na operativni proces ali proces vzdrževanja), je postopek, ki ga je treba upoštevati, opisan v Prilogi I k Izvedbeni uredbi Komisije (EU) 2015/1136 (UL L 185, 14.7.2015, str. 6).
V primeru „pomembne spremembe“ bi moral poročilo o varnostni oceni predlagatelju spremembe predložiti neodvisni „ocenjevalni organ“ (lahko je nacionalni varnostni organ ali drug tehnično usposobljen organ).
Po postopku analize tveganja bo predlagatelj spremembe uporabil ustrezne ukrepe za zmanjšanje tveganj (če je predlagatelj prevoznik v železniškem prometu ali upravljavec infrastrukture, je uporaba uredbe del njegovega sistema upravljanja varnosti, katerega uporabo nadzoruje nacionalni varnostni organ).

sistemom umetne inteligence, da bi ti uresničili cilje, ki jih ljudje določijo[42]. Obstoječa zakonodaja Unije o varnosti proizvodov ne zajema izrecno človeškega nadzora v kontekstu samoučečih se proizvodov in sistemov umetne inteligence[43].

Ustrezni zakonodajni akti Unije lahko kot varovalo predvidijo posebne zahteve za človeški nadzor, in sicer od zasnove proizvoda ter skozi celotni življenjski cikel proizvodov in sistemov umetne inteligence.

Prihodnje „vedenje“ aplikacij umetne inteligence bi lahko povzročilo **tveganje za duševno zdravje**[44] uporabnikov, na primer zaradi interakcije s humanoidnimi roboti in sistemi umetne inteligence doma ali v delovnem okolju. V zvezi s tem se danes pojem varnosti na splošno nanaša na tisto, kar uporabniki občutijo kot tveganja za fizične poškodbe, ki bi lahko nastale zaradi digitalne tehnologije v vzponu. Hkrati so v pravnem okviru EU varni proizvodi opredeljeni kot proizvodi, ki ne predstavljajo tveganja ali pomenijo le minimalno tveganje za varnost in zdravje ljudi. Splošno sprejeto je, da opredelitev zdravja vključuje tako telesno kot duševno dobro počutje. Vendar bi morala biti tveganja za duševno zdravje v zakonodajnem okviru izrecno zajeta v pojmu varnosti proizvodov.

Avtonomnost na primer ne bi smela povzročati čezmernega stresa in neugodja za daljša obdobja ter škodovati duševnemu zdravju. V zvezi s tem se za dejavnike, ki pozitivno vplivajo na občutek varnosti pri starejših[45], štejejo: uspešni odnosi z zaposlenimi v zdravstvu, nadzor nad dnevnimi rutinami in obveščanje o njih. Proizvajalci robotov, ki so v interakciji s starejšimi, bi morali te dejavnike upoštevati pri preprečevanju tveganj za duševno zdravje.

Pri področju uporabe zadevne zakonodaje EU bi lahko razmislili o izrecnih obveznostih za proizvajalce, na primer humanoidnih robotov, ki temeljijo na umetni inteligenci, da bi posebej upoštevali nematerialno škodo, ki bi jo njihovi proizvodi lahko povzročili uporabnikom, zlasti ranljivim uporabnikom, kot so starejši v domovih.

Še ena bistvena značilnost proizvodov in sistemov, ki temeljijo na umetni inteligenci, je **podatkovna odvisnost**. Točnost in ustreznost podatkov je bistvenega pomena za zagotovitev, da sistemi in proizvodi, ki temeljijo na umetni inteligenci, sprejemajo odločitve tako, kot je predvidel proizvajalec.

Zakonodaja Unije o varnosti proizvodov ne obravnava izrecno tveganj za varnost, ki izhajajo iz pomanjkljivih podatkov. Vendar bi morali proizvajalci glede na predvideno „uporabo“ proizvoda že med fazama zasnove in preskušanja predvideti točnost podatkov in njen pomen za varnostne funkcije.

Na primer, sistem, ki temelji na umetni inteligenci in je zasnovan za odkrivanje določenih predmetov, ima lahko težave s prepoznavanjem predmetov v slabih pogojih osvetlitve, zato bi morali načrtovalci vključiti podatke, pridobljene s preskusi proizvodov v običajnih in slabo osvetljenih okoljih.

---

[42] Policy and Investment Recommendations for Trustworthy AI (Politična in naložbena priporočila za zaupanja vredno umetno inteligenco), strokovna skupina na visoki ravni za umetno inteligenco, junij 2019.

[43] Vendar to ne izključuje možnosti, da bo v določenih primerih potreben nadzor zaradi nekaterih obstoječih splošnejših obveznosti v zvezi z dajanjem proizvoda na trg.

[44] Ustanovna listina SZO, prva točka: „Zdravje je stanje popolne fizične, duševne in družbene dobrobiti in ne zgolj stanje brez bolezni ali šibkosti.“ (https://www.who.int/about/who-we-are/constitution)

[45] Social robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction (Socialni roboti: tehnološki, socialni in etični vidiki interakcije med ljudmi in roboti), str. 237–264, Research, Neziha Akalin, Annica Kristoff ersson in Amy Loutfi, julij 2019.

Drug primer se nanaša na kmetijske robote, kot so roboti za pobiranje sadja, ki odkrivajo zrele sadeže na drevesih ali na tleh. Čeprav uporabljeni algoritmi že kažejo več kot 90-odstotno stopnjo uspešnosti pri razvrščanju, bi lahko pomanjkljivosti v podatkovnih nizih, iz katerih črpajo ti algoritmi, vodile k temu, da bi roboti sprejeli slabo odločitev in posledično poškodovali žival ali človeka.

Postavlja se vprašanje, ali bi morala zakonodaja Unije o varnosti proizvodov vsebovati posebne zahteve, ki bi obravnavale tveganja za varnost zaradi pomanjkljivih podatkov v fazi zasnove, ter mehanizme za zagotavljanje, da se kakovost podatkov vzdržuje ves čas uporabe proizvodov in sistemov umetne inteligence.

Nepreglednost je še ena od glavnih značilnosti nekaterih proizvodov in sistemov umetne inteligence, ki lahko nastane zaradi zmožnosti proizvodov in sistemov, da izboljšajo svojo zmogljivost na podlagi učenja iz izkušenj. Glede na metodološki pristop je za proizvode in sisteme, ki temeljijo na umetni inteligenci, značilna različna stopnja nepreglednosti. To lahko privede do tega, da je težko slediti postopku odločanja sistema („učinek črne škatle“). Ljudem morda ni treba razumeti vsake posamezne faze postopka odločanja, vendar je v času, ko so algoritmi umetne inteligence vse bolj napredni in se uporabljajo na kritičnih področjih, zelo pomembno, da so ljudje zmožni razumeti, kako so bile sprejete algoritemske odločitve sistema. To bi bilo še posebej pomembno za naknadni mehanizem izvrševanja, saj bo izvršilnim organom omogočilo spremljati odgovornost ravnanja in izbire sistemov umetne inteligence. To potrjuje tudi sporočilo Komisije o krepitvi zaupanja v umetno inteligenco, osredotočeno na človeka[46].

Zakonodaja Unije o varnosti proizvodov ne obravnava izrecno vse večjih tveganj, ki izhajajo iz nepreglednosti sistemov, ki temeljijo na algoritmih. Zato je treba razmisliti o zahtevah za preglednost algoritmov ter tudi za zanesljivost, odgovornost in, kadar je to ustrezno, človeški nadzor in nepristranske rezultate[47], kar je zlasti pomembno za naknadni mehanizem izvrševanja, in graditi zaupanje v uporabo navedenih tehnologij. Eden od načinov reševanja tega izziva bi bila uvedba obveznosti za razvijalce algoritmov, da v primeru nesreč razkrijejo parametre zasnove in metapodatke o podatkovnih nizih.

Dodatna tveganja, ki bi lahko vplivala na varnost, so tista, ki izhajajo iz **kompleksnosti proizvodov in sistemov**, saj so lahko različni sestavni deli, naprave in proizvodi povezani in vplivajo na delovanje drug drugega (npr. proizvodi, ki so del pametnega domačega ekosistema).

Ta kompleksnost je že obravnavana v pravnem okviru Unije za varnost proizvodov, ki je omenjen na začetku tega oddelka[48]. Zlasti mora proizvajalec pri oceni tveganja za proizvod upoštevati predvideno uporabo, predvidljivo uporabo in, kjer je to primerno, razumno predvidljivo napačno uporabo.

Če proizvajalec predvidi, da bo naprava medsebojno povezana in bo komunicirala z drugimi napravami, bi bilo treba to upoštevati pri oceni tveganja. Uporaba ali napačna uporaba se na primer določi na podlagi izkušenj z uporabo enake vrste proizvoda v preteklosti, preiskav nesreč ali človeškega vedenja.

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

[47] Na podlagi ključnih zahtev, ki jih je predlagala strokovna skupina na visoki ravni v etičnih smernicah za zaupanja vredno umetno inteligenco: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines.

[48] Uredba (ES) št. 2008/765 in Sklep (ES) št. 2008/768 ter harmonizirana sektorska zakonodaja o varnosti proizvodov, npr. Direktiva 2006/42/ES o strojih.

Kompleksnost sistemov je podrobneje obravnavana tudi v sektorski zakonodaji o varnosti proizvodov, kot je uredba o medicinskih pripomočkih, in do določene mere v zakonodaji o splošni varnosti proizvodov[49]. Na primer, proizvajalec povezane naprave, ki naj bi bila del pametnega domačega ekosistema, bi moral biti zmožen razumno predvideti, da bodo njegovi proizvodi vplivali na varnost drugih proizvodov.

Poleg tega zakonodaja o prometu obravnava to kompleksnost na sistemski ravni. Za avtomobile, vlake in letala se homologacija in certificiranje izvajata za vsak sestavni del ter za celotno vozilo ali zrakoplov. Tehnična ustreznost vozil in zrakoplovov ter interoperabilnost železniškega sistema sta vključeni v oceno varnosti. V prometu mora „sisteme“ „odobriti“ organ, in sicer bodisi na podlagi ocene skladnosti z jasno določenimi tehničnimi zahtevami, ki jo izvede tretja stran, ali po predstavitvi obravnavanja tveganj. Rešitev je na splošno kombinacija ravni „proizvoda“ in „sistema“.

Zakonodaja Unije o varnosti proizvodov, vključno s prometno zakonodajo, v določeni meri že upošteva kompleksnost proizvodov ali sistemov, da bi odpravila tveganja, ki bi lahko vplivala na varnost uporabnikov.

Kompleksni sistemi pogosto vključujejo **programsko opremo**, ki je bistven sestavni del sistema, ki temelji na umetni inteligenci. Na splošno mora proizvajalec končnega proizvoda v prvotni oceni tveganja predvideti tveganja v zvezi s programsko opremo, ki je integrirana v proizvod ob dajanju na trg.

Nekateri deli zakonodaje Unije o varnosti proizvodov se izrecno sklicujejo na programsko opremo, ki je integrirana v proizvod. Direktiva o strojih[50] na primer zahteva, da napaka programske opreme krmilnega sistema ne sme povzročiti nevarnih situacij.

V zakonodaji Unije o varnosti proizvodov je posodobitve programske opreme mogoče primerjati z vzdrževalnimi ukrepi iz varnostnih razlogov, če bistveno ne spreminjajo proizvoda, ki je že bil dan na trg, in ne prinašajo novih tveganj, ki niso bila predvidena v prvotni oceni tveganja. Če pa posodobitev programske opreme bistveno spremeni proizvod, v katerega se naloži, se lahko celoten proizvod šteje za nov proizvod, pri čemer je treba skladnost z ustrezno zakonodajo o varnostni proizvodov ponovno oceniti, ko se izvede sprememba[51].

Harmonizirana sektorska zakonodaja Unije o varnosti proizvodov za posamezne sektorje na splošno ne vsebuje posebnih določb za samostojno programsko opremo, dano na trg kot tako ali naloženo po tem, ko je bil na trg dan proizvod. Vendar nekateri deli zakonodaje Unije obravnavajo samostojno programsko opremo, na primer uredba o medicinskih pripomočkih. Poleg tega se samostojna programska oprema, naložena v povezane proizvode, ki komunicirajo prek nekaterih radijskih modulov[52], z delegiranimi akti lahko ureja tudi na podlagi direktive o radijski opremi. Navedena direktiva zahteva, da posebni razredi ali kategorije radijske opreme podpirajo funkcije, ki zagotavljajo, da pri nalaganju programske opreme ni ogrožena skladnost te opreme[53].

---

[49] V členu 2 direktive o splošni varnosti proizvodov je določeno, da varen proizvod upošteva „vpliv na druge proizvode, kadar se razumno predvideva, da bo uporabljen skupaj z drugimi proizvodi“.

[50] Oddelek 1.2.1 Priloge I k Direktivi o strojih.

[51] Modri vodnik za izvajanje predpisov EU o proizvodih, 2016.

[52] Radijski moduli so elektronske naprave, ki prenašajo in/ali sprejemajo radijske signale (WIFI, Bluetooth) med dvema napravama.

[53] Člen 3(3)(i) direktive o radijski opremi.

Zakonodaja Unije o varnosti proizvodov upošteva varnostna tveganja, ki izhajajo iz programske opreme, integrirane v proizvod ob njegovem dajanju na trg, in morebitnih naknadnih posodobitev, ki jih predvidi proizvajalec, vendar pa bi lahko bile potrebne posebne in/ali izrecne zahteve glede samostojne programske opreme (npr. „aplikacij“, ki se prenesejo). Posebno pozornost bi bilo treba nameniti samostojni programski opremi, ki zagotavlja varnostne funkcije v proizvodih in sistemih umetne inteligence.

Morda bodo potrebne dodatne obveznosti za proizvajalce, da se zagotovi, da bodo poskrbeli za funkcije za preprečevanje nalaganja programske opreme, ki vpliva na varnost, med življenjsko dobo proizvodov umetne inteligence.

Na digitalne tehnologije v vzponu pa vplivajo tudi **kompleksne vrednostne verige**. Vendar ta kompleksnost ni nova niti ne gre zgolj za vprašanje, ki bi ga prinesle digitalne tehnologije v vzponu, kot sta umetna inteligenca ali internet stvari. To velja na primer za proizvode, kot so računalniki, strežni roboti ali prevozni sistemi.

V okviru Unije za varnost proizvodov ostaja odgovornost za varnost proizvoda na strani proizvajalca, ki da proizvod na trg, ne glede na to, kako kompleksna je vrednostna veriga. Proizvajalci so odgovorni za varnost končnega proizvoda, vključno z deli, vgrajenimi v proizvod, npr. programsko opremo računalnika.

Nekateri deli zakonodaje Unije o varnosti proizvodov že vsebujejo določbe, ki se izrecno nanašajo na primere, ko v določen proizvod posega več gospodarskih subjektov, preden se ta da na trg. Direktiva o dvigalih[54] na primer zahteva, da gospodarski subjekt, ki načrtuje in izdela dvigalo, monterju[55] zagotovi „*vse potrebne dokumente in informacije, da ji omogoči zagotovitev pravilne in varne montaže in preskušanja dvigala*“. Direktiva o strojih zahteva, da proizvajalci opreme upravljavcu zagotovijo informacije o montiranju te opreme na druge stroje[56].

Zakonodaja Unije o varnosti proizvodov upošteva kompleksnost vrednostnih verig in nalaga obveznosti za več gospodarskih subjektov na podlagi načela „deljene odgovornosti“.

Odgovornost proizvajalca za varnost končnih proizvodov se je izkazala kot primerna za sedanje kompleksne vrednostne verige, vendar bi lahko izrecne določbe, ki bi posebej zahtevale sodelovanje med gospodarskimi subjekti v dobavni verigi in uporabniki, zagotovile pravno varnost v morda še bolj kompleksnih vrednostnih verigah. Zlasti bi vsak akter v vrednostni verigi, ki ima vpliv na varnost proizvoda (npr. proizvajalci programske opreme) in uporabnik (ki spremeni proizvod), prevzel odgovornost ter naslednjemu akterju v vrednostni verigi sporočil potrebne informacije in ukrepe.

3. Odgovornost

Na ravni Unije določbe o varnosti proizvodov in odgovornosti za proizvode predstavljajo dopolnjujoča se mehanizma za uresničitev istega cilja politike, in sicer delujočega enotnega

[54] V skladu s členom 16(2) Direktive 2014/33/EU.

[55] V Direktivi 2014/33/EU o dvigalih je monter enakovreden proizvajalcu in mora prevzeti odgovornost za zasnovo, proizvodnjo, montažo in dajanje na trg dvigala.

[56] Direktiva o strojih, Priloga I, člen 1.7.4.2: „*Vsaka navodila za uporabo morajo, kadar je ustrezno, vsebovati vsaj naslednje informacije:*“ „*(i) navodila za sestavljanje, namestitev in priključitev, vključno z risbami, diagrami in pritrdilnimi sredstvi ter določitev podstavka ali napeljave, na katero mora biti stroj nameščen*“.

trga za blago, ki zagotavlja visoko raven varnosti, tj. da se čim bolj zmanjšajo tveganja škode za uporabnike in zagotovijo nadomestila za škodo, ki je posledica blaga z napako.

Na nacionalni ravni neharmonizirani okviri civilne odgovornosti dopolnjujejo ta pravila Unije, tako da zagotavljajo nadomestilo za škodo iz različnih razlogov (npr. za proizvode in storitve) in obravnavajo različne odgovorne osebe (npr. lastnike, upravljavce ali ponudnike storitev).

Čeprav se je z optimizacijo predpisov Unije o varnosti za umetno inteligenco mogoče izogniti nesrečam, se te lahko kljub vsemu zgodijo. Takrat se uporabi civilna odgovornost. Pravila o civilni odgovornosti imajo v naši družbi dvojno vlogo: po eni strani zagotavljajo, da žrtve škode, ki so jo povzročili drugi, dobijo odškodnino, po drugi strani pa dajejo ekonomske spodbude odgovorni osebi, da bi se izognila povzročitvi take škode. Pravila o odgovornosti morajo vedno najti ravnotežje med zaščito državljanov pred škodo ter omogočanjem, da podjetja sprejemajo inovacije.

Okviri odgovornosti v Uniji delujejo dobro. Opirajo se na vzporedno uporabo direktive o odgovornosti za proizvode (Direktiva 85/374/EGS), ki je harmonizirala odgovornost proizvajalca proizvodov z napako, in drugih neharmoniziranih nacionalnih ureditev odgovornosti.

Direktiva o odgovornosti za proizvode zagotavlja zaščito na ravni, ki je nacionalna pravila o krivdni odgovornosti sama po sebi ne pokrivajo. Uvaja sistem objektivne odgovornosti proizvajalca za škodo, ki je nastala zaradi napake na njihovih proizvodih. V primeru fizične ali materialne škode ima oškodovanec pravico do odškodnine, če dokaže škodo, napako na proizvodu (tj. da proizvod ni zagotovil varnosti, ki jo javnost upravičeno pričakuje) in vzročno zvezo med proizvodom z napako in škodo.

Nacionalne neharmonizirane ureditve zagotavljajo pravila o krivdni odgovornosti, v skladu s katerimi morajo oškodovanci za uspešno odškodninsko terjatev dokazati krivdo odgovorne osebe, škodo in vzročno zvezo med napako in škodo. Prav tako določajo režime objektivne odgovornosti, kadar nacionalni zakonodajalec odgovornost za tveganje pripiše določeni osebi, pri čemer oškodovancu ni treba dokazati krivde/napake ali vzročne zveze med krivdo/napako in škodo.

Nacionalne ureditve odgovornosti žrtvam škode, ki so jo povzročili proizvodi in storitve, ponujajo možnost več vzporednih odškodninskih zahtevkov, ki temeljijo na krivdni ali objektivni odgovornosti. Ti zahtevki so pogosto naslovljeni na različne odgovorne osebe in zanje veljajo drugačni pogoji.

Na primer, oškodovanec, udeležen v avtomobilski nesreči, lahko običajno vloži zahtevek za ugotovitev objektivne odgovornosti lastnika vozila (tj. osebe, ki sklene zavarovanje avtomobilske odgovornosti) in zahtevek za ugotovitev krivdne odgovornosti voznika, oba v skladu z nacionalnim civilnim pravom, v skladu z direktivo o odgovornosti za proizvode pa poleg tega tudi zahtevek proti proizvajalcu, če je imel avtomobil napako.

V skladu s harmoniziranimi pravili o zavarovanju za motorna vozila mora biti uporaba vozila zavarovana[57], zavarovatelj pa je v praksi vedno prvi, na katerega se naslovi odškodninski zahtevek za telesno poškodbo ali materialno škodo. V skladu s temi pravili obvezno zavarovanje oškodovancu zagotavlja nadomestilo in ščiti zavarovano osebo, ki je po

[57] Za motorna vozila harmonizirano z Direktivo 2009/103/ES o zavarovanju civilne odgovornosti pri uporabi motornih vozil in o izvajanju obveznosti zavarovanja takšne odgovornosti.

nacionalnih predpisih civilnega prava[58] odgovorna za plačilo denarne odškodnine za prometno nesrečo, v kateri je bilo udeleženo motorno vozilo. Za proizvajalce se v skladu z direktivo o odgovornosti za proizvode ne uporablja obvezno zavarovanje. Kar zadeva zavarovanje motornih vozil, avtonomna vozila v zakonodaji EU niso obravnavana drugače kot neavtonomna. Za taka vozila mora biti kot za vsa vozila sklenjeno zavarovanje avtomobilske odgovornosti za škodo, povzročeno tretjim osebam, ki za oškodovanca predstavlja najlažji način, da prejme nadomestilo.

Z ustreznim zavarovanjem se lahko ublažijo negativne posledice nesreč, tako da se nemoteno zagotovi odškodnina za oškodovance. Jasna pravila o odgovornosti zavarovalnicam pomagajo izračunati tveganja in od stranke, ki je dejansko odgovorna za škodo, zahtevati povračilo. Če je na primer nesreča povzročena zaradi napake v vozilu, lahko zavarovatelj motornega vozila po izplačilu odškodnine oškodovancu zahteva povračilo od proizvajalca.

Vendar značilnosti digitalnih tehnologij v vzponu, kot so umetna inteligenca, internet stvari in robotika, ogrožajo nekatere vidike okvirov za odgovornost na ravni Unije in nacionalni ravni ter bi lahko zmanjšale njihovo učinkovitost. Nekatere od teh značilnosti bi lahko povzročile, da bi bilo škodo težko povezati s človeškim ravnanjem, kar bi lahko bila podlaga za zahtevek za ugotavljanje krivdne odgovornosti v skladu z nacionalnimi pravili. To pomeni, da bi lahko bilo utemeljevanje odškodninskih zahtevkov na podlagi nacionalne odškodninske zakonodaje težavno ali predrago, oškodovanci pa posledično morda ne bi mogli prejeti ustrezne odškodnine. Pomembno je, da žrtve nesreč, ki so povezane s proizvodi in storitvami, ki vključujejo digitalne tehnologije v vzponu, kot je umetna inteligenca, niso deležni nižje ravni varstva kot žrtve nesreč, povezanih s podobnimi drugimi proizvodi in storitvami, za katere bi dobili odškodnino na podlagi nacionalne odškodninske zakonodaje. To bi lahko zmanjšalo družbeno sprejemljivost navedenih novih tehnologij in povzročilo, da bi jih ljudje uporabljali z oklevanjem.

Treba bo oceniti, ali bi lahko izzivi, ki jih predstavljajo nove tehnologije za obstoječe okvire, povzročili tudi pravno negotovost glede uporabe obstoječe zakonodaje (npr. kako bi se pojem krivde uporabljal za škodo, ki jo je povzročila umetna inteligenca). To bi lahko zaviralo naložbe ter povečalo stroške obveščanja in zavarovanja za proizvajalce in druga podjetja v dobavni verigi, zlasti evropska MSP. Če bi države članice nazadnje obravnavale izzive, s katerimi se soočajo nacionalni okviri za odgovornost, bi to poleg tega lahko privedlo do nadaljnje razdrobljenosti, s čimer bi se povečali stroški za uvajanje inovativnih rešitev na podlagi umetne inteligence in zmanjšala čezmejna trgovina na enotnem trgu. Pomembno je, da podjetja poznajo tveganja v zvezi z odgovornostjo v celotni vrednostni verigi in jih lahko zmanjšajo ali preprečijo ter se pred njimi zavarujejo.

To poglavje pojasnjuje, kako nove tehnologije na preizkušnjo postavljajo obstoječe okvire in kako bi lahko obravnavali te izzive. Poleg tega bi bilo treba posebej razmisliti o posebnostih nekaterih sektorjev, na primer zdravstvenega.

Kompleksnost proizvodov, storitev in vrednostne verige: v zadnjih desetletjih sta se tehnologija in industrija močno razvili. Zlasti ločnica med proizvodi in storitvami ni več tako jasna, kot je bila. Proizvodi in zagotavljanje storitev se vse bolj prepletajo. Čeprav kompleksni proizvodi in vrednostne verige za evropsko industrijo ali njen regulativni model niso novi, pa si programska oprema in umetna inteligenca zaslužita posebno pozornost, ko gre za odgovornost za proizvode. Programska oprema je bistvena za delovanje številnih

[58] V večini držav članic se za osebo, v imenu katere je registrirano motorno vozilo, uporablja objektivna odgovornost.

proizvodov in lahko vpliva na njihovo varnost. Integrirana je v proizvode, lahko pa se dobavlja tudi ločeno, da se omogoči predvidena uporaba proizvoda. Niti računalnik niti pametni telefon ne bi bila posebno uporabna brez programske opreme. To pomeni, da lahko programska oprema povzroči napako na oprijemljivem proizvodu in posledično fizično škodo (glej okvir o programski opremi v poglavju o varnosti). To bi posledično spet pomenilo odgovornost proizvajalca na podlagi direktive o odgovornosti za proizvode.

Ker pa obstajajo številne različne vrste in oblike programske opreme, je ni vedno enostavno razvrstiti bodisi kot storitev bodisi kot proizvod. Medtem ko bi programsko opremo, ki usmerja delovanje oprijemljivega proizvoda, lahko razumeli kot element ali sestavni del tega proizvoda, je nekatere oblike samostojne programske opreme težje razvrstiti.

Čeprav je opredelitev proizvoda iz direktive o odgovornosti za proizvode široka, bi se njeno področje uporabe lahko še podrobneje opredelilo, da bi se bolje odražala kompleksnost tehnologij v vzponu in zagotovilo, da je odškodnina vedno na voljo za škodo, ki jo povzročijo proizvodi, ki imajo napako zaradi programske opreme ali drugih digitalnih funkcij. To bi gospodarskim subjektom, kot so razvijalci programske opreme, omogočilo, da bolje ocenijo, ali bi se jih lahko štelo za proizvajalce v skladu z direktivo o odgovornosti za proizvode.

Aplikacije umetne inteligence so pogosto povezane v **kompleksnih okoljih interneta stvari**, v katerih medsebojno delujejo številne različne povezane naprave in storitve. Združevanje različnih digitalnih komponent v kompleksnem ekosistemu in pluralnost vpletenih akterjev lahko oteži oceno, kaj je izvor morebitne škode in katera oseba je zanjo odgovorna. Zaradi kompleksnosti teh tehnologij je za oškodovance morda zelo težko identificirati odgovorno osebo in dokazati vsa potrebna dejstva za uspešno terjatev, kot to zahteva nacionalna zakonodaja. Stroški dokazovanja so lahko ekonomsko nevzdržni in oškodovance odvračajo od uveljavljanja odškodnine.

Poleg tega bodo proizvodi in storitve, ki temeljijo na umetni inteligenci, delovali skupaj s tradicionalnimi tehnologijami, kar bo povzročilo dodatno zapletenost tudi v zvezi z odgovornostjo. Avtonomni avtomobili si bodo na primer v nekem trenutku delili cesto s tradicionalnimi vozili. V nekaterih storitvenih sektorjih (kot so upravljanje prometa in zdravstveno varstvo), kjer bodo delno avtomatizirani sistemi umetne inteligence podpirali človekove odločitve, se bo pojavila podobna kompleksnost medsebojno delujočih akterjev.

V skladu s poročilom[59] podskupine za nove tehnologije v okviru strokovne skupine za odgovornost in nove tehnologije bi veljalo razmisliti o prilagoditvi nacionalnih zakonov za olajšanje dokaznega bremena žrtev škode, povezane z umetno inteligenco. Dokazno breme bi bilo na primer lahko vezano na skladnost (s strani zadevnega izvajalca) s posebnimi obveznostmi v zvezi s kibernetsko varnostjo ali drugimi varnostnimi zahtevami, določenimi z zakonom: v primeru nespoštovanja teh pravil bi se lahko dokazno bremene glede krivde in vzročne zveze preložilo na nasprotno stran.

Komisija si prizadeva pridobiti mnenja o tem, ali in v kakšnem obsegu bo morda treba ublažiti posledice kompleksnosti z lajšanjem/preložitvijo dokaznega bremena, ki ga zahtevajo nacionalni predpisi o odgovornosti za škodo, nastalo zaradi delovanja aplikacij umetne inteligence, in sicer na podlagi ustrezne pobude EU.

[59] Liability for Artificial Intelligence and other emerging technologies' Report (Poročilo o odgovornosti za umetno inteligenco in druge tehnologije v vzponu): https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

Kar zadeva zakonodajo Unije, bi se v skladu z direktivo o odgovornosti za proizvode za proizvod, ki ne izpolnjuje obveznih varnostnih predpisov, štelo, da ima napako, ne glede na krivdo proizvajalcev. Obstajajo pa lahko tudi razlogi za razmislek o tem, kako olajšati dokazno breme za oškodovance v skladu z Direktivo: direktiva se opira na nacionalne predpise o dokazovanju in na določitev vzročne zveze.

Povezljivost in odprtost: Trenutno ni povsem jasno, kakšna bi lahko bila pričakovanja glede varnosti v zvezi s škodo, ki izhaja iz kršitev kibernetske varnosti v proizvodih, in ali bi bila odškodnina za tako škodo ustrezno povrnjena v skladu z direktivo o odgovornosti za proizvode.

Težave na področju kibernetske varnosti lahko obstajajo že od samega začetka, ko je proizvod dan v promet, lahko pa se pojavijo tudi precej pozneje.

V okvirih krivdne odgovornosti določitev jasnih obveznosti glede kibernetske varnosti operaterjem omogoča, da ugotovijo, kaj morajo storiti, da bi se izognili posledicam odgovornosti.

V skladu z direktivo o odgovornosti za proizvode bi vprašanje, ali bi lahko proizvajalec predvidel nekatere spremembe ob upoštevanju razumno predvidljive uporabe proizvoda, lahko postalo pomembnejše. Lahko bi na primer prišlo do pogostejšega sklicevanja na „pozneje nastalo napako“, pri čemer proizvajalec ni odgovoren, če napaka ni obstajala v času, ko je bil proizvod dan v promet, ali na „razvojno tveganje“ (tj. da s takratnim tehničnim znanjem ni bilo mogoče predvideti napake). Poleg tega bi se lahko zmanjšala odgovornost, če oškodovanec ne bi izvajal posodobitev, pomembnih za varnost. To bi se potencialno lahko štelo za malomarno ravnanje oškodovanca, s čimer bi se zmanjšala odgovornost proizvajalca. Ker lahko pojem razumno predvidljive uporabe in vprašanje malomarnosti oškodovanca, kot je neprenos varnostne posodobitve, postaneta bolj pomembna, se lahko zgodi, da bodo oškodovanci težje prišli do nadomestila za škodo, ki je nastala zaradi napake proizvoda.

Avtonomnost in nepreglednost: kadar so aplikacije umetne inteligence sposobne delovati avtonomno, opravljajo nalogo, pri kateri ni vsak korak vnaprej določen, in to z manj, nazadnje pa tudi popolnoma brez neposrednega človeškega nadzora. Algoritme, ki temeljijo na strojnem učenju, je včasih težko, skoraj nemogoče razumeti (tako imenovani „učinek črne škatle“).

Poleg kompleksnosti, ki je bila obravnavana zgoraj, je lahko pridobitev nadomestila za škodo, ki so jo povzročile avtonomne aplikacije umetne inteligence, oteženo tudi zaradi učinka črne škatle v zvezi z nekaterimi aplikacijami umetne inteligence. Potreba po razumevanju algoritma in podatkov, ki jih uporablja umetna inteligenca, zahteva analitično in tehnično strokovno znanje, ki bi bilo za oškodovance lahko predrago. Poleg tega dostop do algoritmov in podatkov ne bi bil mogoč brez sodelovanja potencialno odgovorne stranke. V praksi oškodovanci torej morda ne bi mogli uveljavljati odškodninskega zahtevka. Poleg tega ne bi bilo jasno, kako dokazati krivdo, kadar umetna inteligenca deluje avtonomno, ali kaj se šteje za napako osebe, ki se zanaša na uporabo umetne inteligence.

Nacionalne zakonodaje so že razvile številne rešitve za zmanjšanje dokaznega bremena za oškodovance v podobnih primerih.

Vodilno načelo Unije za varnost proizvodov in odgovornost za proizvode ostaja, da so proizvajalci tisti, ki morajo zagotoviti, da so vsi proizvodi, dani na trg, varni skozi celoten življenjski cikel ter ob uporabi proizvoda, ki jo je mogoče razumno predvideti. To pomeni, da bi moral proizvajalec zagotoviti, da je proizvod, ki uporablja umetno inteligenco, skladen z določenimi varnostnimi parametri. Značilnosti umetne inteligence ne izključujejo pravice

potrošnikov, da pričakujejo varen proizvod, ne glede na to, ali gre za samodejne kosilnice ali kirurške robote.

Avtonomnost lahko vpliva na varnost proizvoda, saj lahko bistveno spremeni lastnosti proizvoda, vključno z njegovimi varnostnimi značilnostmi. Gre za vprašanje, pod kakšnimi pogoji funkcije samoučenja podaljšujejo odgovornost proizvajalca in v kolikšni meri bi moral proizvajalec predvideti določene spremembe.

Ob natančnem upoštevanju ustreznih sprememb v okviru Unije za varnost proizvodov bi se lahko pojem „dajanje v promet“, ki se trenutno uporablja v direktivi o odgovornosti za proizvode, ponovno proučil, da bi se upoštevalo dejstvo, da se proizvodi lahko spremenijo. To bi lahko tudi pomagalo pojasniti, kdo je odgovoren za morebitne spremembe proizvoda.

V skladu s poročilom[60] podskupine za nove tehnologije v okviru skupine strokovnjakov za odgovornost in nove tehnologije bi lahko imelo delovanje nekaterih avtonomnih naprav in storitev umetne inteligence poseben profil tveganja v smislu odgovornosti, saj bi lahko povzročile znatno škodo za pomembne pravne interese, kot so življenje, zdravje in premoženje, ter bi široko javnost izpostavile tveganjem. To bi lahko zadevalo predvsem naprave umetne inteligence, ki se premikajo po javnih območjih (npr. popolnoma avtonomna vozila, brezpilotni zrakoplovi[61] ali roboti za dostavo paketov) ali storitve, ki temeljijo na umetni inteligenci in prinašajo podobna tveganja (npr. storitve upravljanja prometa, ki usmerjajo ali nadzorujejo vozila ali upravljanje distribucije električne energije). Izzivi, ki jih za nacionalne odškodninske zakone prinašata avtonomnost in nepreglednost, bi se lahko obravnavali na podlagi pristopa, ki temelji na tveganju. S shemami objektivne odgovornosti bi se lahko zagotovilo, da oškodovanec v primeru, da se to tveganje uresniči, prejme nadomestilo ne glede na krivdo. Treba bi bilo skrbno oceniti, kako odločitev, kdo bi moral biti v takih primerih objektivno odgovoren, vpliva na razvoj in uvajanje umetne inteligence, ter upoštevati pristop, ki temelji na tveganju.

Komisija želi v zvezi z delovanjem aplikacij umetne inteligence s posebnim profilom tveganja pridobiti mnenja o tem, ali in v kakšni meri bi lahko bila za to, da morebitni oškodovanci prejmejo učinkovito odškodnino, potrebna objektivna odgovornost, kakršna obstaja v nacionalnih zakonodajah za podobna tveganja, ki jim je izpostavljena javnost (na primer za upravljanje motornih vozil, letal ali jedrskih elektrarn). Komisija prav tako zbira mnenja o združitvi objektivne odgovornosti z morebitno obveznostjo sklenitve razpoložljivega zavarovanja na podlagi primera iz direktive o avtomobilskem zavarovanju, da bi se zagotovila odškodnina ne glede na solventnost odgovorne osebe in zmanjšali stroški škode.

Za delovanje vseh drugih aplikacij umetne inteligence, ki bi predstavljale veliko večino, Komisija preučuje, ali je treba prilagoditi dokazno breme glede vzročne zveze in napake. V zvezi s tem se eno od vprašanj iz poročila[62] podskupine za nove tehnologije v okviru skupine strokovnjakov za odgovornost in nove tehnologije nanaša na primer, ko potencialno

[60] Liability for Artificial Intelligence and other emerging technologies' Report (Poročilo o odgovornosti za umetno inteligenco in druge tehnologije v vzponu): https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

[61] Sistemi brezpilotnih zrakoplovov iz Izvedbene uredbe Komisije (EU) 2019/947 z dne 24. maja 2019 o pravilih in postopkih za upravljanje brezpilotnih zrakoplovov.

[62] Liability for Artificial Intelligence and other emerging technologies' Report (Poročilo o odgovornosti za umetno inteligenco in druge tehnologije v vzponu): https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

odgovorna stran ni zabeležila podatkov, ki so pomembni za oceno odgovornosti ali jih ni pripravljena deliti z oškodovancem.

4. Zaključek

Pojav novih digitalnih tehnologij, kot so umetna inteligenca, internet stvari in robotika, prinaša nove izzive v smislu varnosti in odgovornosti za proizvode, na primer v zvezi s povezljivostjo, avtonomnostjo, podatkovno odvisnostjo, nepreglednostjo, kompleksnostjo proizvodov in sistemov, posodobitvami programske opreme in bolj zapletenim varnostnim upravljanjem in vrednostnimi verigami.

Veljavna zakonodaja o varnosti proizvodov vsebuje številne vrzeli, ki jih je treba odpraviti, zlasti v direktivi o splošni varnosti proizvodov, direktivi o strojih, direktivi o radijski opremi in novem zakonodajnem okviru. Prihodnje delo v zvezi s prilagoditvijo različnih zakonodajnih aktov v tem okviru bo potekalo dosledno in usklajeno.

Novi izzivi na področju varnosti ustvarjajo tudi nove izzive glede odgovornosti. Te izzive je treba obravnavati, da se zagotovi enaka raven varstva v primerjavi z žrtvami škode, ki jo povzročijo tradicionalne tehnologije, hkrati pa ohrani ravnotežje s potrebami po tehnoloških inovacijah. To bo pomagalo ustvariti zaupanje v digitalne tehnologije v vzponu in naložbeno stabilnost.

Medtem ko se obstoječi predpisi na področju odgovornosti na ravni Unije in na nacionalni ravni načeloma lahko uporabljajo za tehnologije v vzponu, bi lahko razsežnost in skupni učinek izzivov, ki jih prinaša umetna inteligenca, otežila uveljavljanje odškodnine za oškodovance v vseh upravičenih primerih[63]. Dodelitev stroškov v primeru škode je tako v skladu z veljavnimi pravili lahko nepoštena ali neučinkovita. Da bi to popravili in odpravili morebitne negotovosti v obstoječem okviru, bi lahko razmislili o nekaterih prilagoditvah direktive o odgovornosti za proizvode in nacionalnih ureditvah odgovornosti s primernimi pobudami EU, ki bi sledile ciljno usmerjenemu, na tveganju temelječem pristopu, tj. ob upoštevanju dejstva, da različne aplikacije umetne inteligence predstavljajo različna tveganja.

[63] Glej poročilo podskupine za nove tehnologije, str. 3, in priporočilo politike 27.2 strokovne skupine na visoki ravni za umetno inteligenco.