

V Bruseli 19. 2. 2020
COM(2020) 64 final

**SPRÁVA KOMISIE EURÓPSKEMU PARLAMENTU, RADE A EURÓPSKEMU
HOSPODÁRSKEMU A SOCIÁLNE MU VÝBORU**

**Správa o vplyve umelej inteligencie, internetu vecí a robotiky na bezpečnosť
a zodpovednosť**

SPRÁVA O VPLYVE UMELEJ INTELIGENCIE, INTERNETU VECÍ A ROBOTIKY NA BEZPEČNOSŤ A ZODPOVEDNOSŤ

1. Úvod

Umelá inteligencia (UI)¹, internet vecí² a robotika prinesú našej spoločnosti nové príležitosti a výhody. Komisia uznáva význam a potenciál týchto technológií aj potrebu významných investícií v týchto oblastiach.³ Je odhodlaná urobiť z Európy v oblasti umelej inteligencie, internetu vecí a robotiky svetového lídra. Na dosiahnutie tohto cieľa je potrebný jasný a predvídateľný právny rámec, ktorý si poradí s technologickými výzvami.

1.1. Súčasný rámec bezpečnosti a zodpovednosti

Právne rámce týkajúce sa bezpečnosti a zodpovednosti majú celkovo zabezpečiť, aby všetky výrobky a služby vrátane tých, do ktorých sú zabudované nové digitálne technológie, fungovali bezpečne, spoľahlivo a konzistentne a ak dôjde k ujme, aby bola účinne napravená. Vysoká úroveň bezpečnosti výrobkov a systémov, do ktorých sú zabudované nové digitálne technológie, a spoľahlivé mechanizmy odškodnenia (t. j. rámec zodpovednosti) prispievajú k lepšej ochrane spotrebiteľov. Zároveň sa vďaka tomu vybuduje dôvera v tieto technológie, bez ktorej by ich priemysel a používatelia neprijali. To na druhej strane posilní konkurencieschopnosť nášho priemyslu a napomôže dosiahnuť ciele Únie⁴. Jasný rámec bezpečnosti a zodpovednosti je najmä v prípade nových technológií, ako je umelá inteligencia, internet vecí a robotika, mimoriadne dôležitý, a to tak pre ochranu spotrebiteľov, ako aj pre právnu istotu podnikov.

Únia má v oblasti bezpečnosti a zodpovednosti za výrobky pevný a spoľahlivý regulačný rámec a rozsiahly súbor bezpečnostných noriem, ktoré dopĺňajú vnútroštátne a neharmonizované právne predpisy v oblasti zodpovednosti. Spoločne zabezpečujú blahobyt našich občanov a podporujú inovácie a využívanie technológií na jednotnom trhu. Umelá inteligencia, internet vecí a robotika však vlastnosti mnohých výrobkov a služieb menia.

V oznámení o umelej inteligencii pre Európu⁵, ktoré bolo prijaté 25. apríla 2018, sa uvádza, že Komisia predloží správu, v ktorej posúdi vplyv nových digitálnych technológií na existujúce rámce bezpečnosti a zodpovednosti. Táto správa má za úlohu identifikovať a preskúmať širšie dôsledky a možné medzery v rámcoch zodpovednosti a bezpečnosti pre umelú inteligenciu, internet vecí a robotiku. Táto správa slúži ako sprievodný dokument k bielej knihe o umelej inteligencii a predkladá východiská na diskusiu, ktoré sú súčasťou širšej konzultácie so zainteresovanými stranami. Časť venovaná bezpečnosti vychádza

¹ Vymedzenie umelej inteligencie, ako ho predložila expertná skupina na vysokej úrovni pre umelú inteligenciu, je k dispozícii na adrese <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>.

² Internet vecí je vymedzený v odporúčaní ITU-T Y.2060 dostupnom na adrese <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>.

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

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

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

V sprievodnom pracovnom dokumente útvarov Komisie (2018) 137 (<https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137>) bolo prvýkrát zmapované, aké výzvy prinášajú v súvislosti so zodpovednosťou nové digitálne technológie.

z hodnotenia⁶ smernice o strojových zariadeniach⁷ a z práce s príslušnými expertnými skupinami⁸. Časť venovaná zodpovednosti vychádza z hodnotenia⁹ smernice o zodpovednosti za výrobky¹⁰, príspevkov príslušných expertných skupín¹¹ a kontaktov so zainteresovanými stranami. Cieľom tejto správy nie je poskytnúť vyčerpávajúci prehľad existujúcich pravidiel bezpečnosti a zodpovednosti, ale zamerať sa na doteraz zistené kľúčové problémy.

1.2. Vlastnosti umelej inteligencie, internetu vecí a robotických technológií

Umelá inteligencia, internet vecí a robotika majú mnoho spoločných vlastností. Spája sa v nich **prepojitelnosť**, **autonómnosť** a **závislosť od údajov** a plnia úlohy viac-menej bez ovládania človekom či ľudského dohľadu. Systémy umelej inteligencie dokážu na základe skúsenosti zlepšovať vlastnú výkonnosť. Vzhľadom na rôznorodosť hospodárskych subjektov zapojených do **dodávateľského reťazca**, ako aj rozmanitosť komponentov, častí, softvéru, systémov alebo služieb, ktoré spolu vytvárajú nové technologické ekosystémy, sa vyznačujú **zložitosťou**. Navyše po uvedení na trh sú **otvorené** aktualizáciám a novým verziám. Keďže ide obrovské množstvo údajov, systém sa spolieha na algoritmy a rozhodovanie v oblasti umelej inteligencie je **neprieľadné**, ťažšie možno predvídať správanie výrobku vybaveného umelou inteligenciou a pochopiť možné príčiny ujmy. A napokon prepojitelnosť a otvorenosť môže výrobky umelej inteligencie a internetu vecí vystaviť **kybernetickým hrozbám**.

1.3. Umelá inteligencia, internet vecí a robotika prinášajú príležitosti

Umelá inteligencia, internet vecí a robotika prinášajú okrem iného príležitosť zvýšiť dôveru používateľov v nové technológie aj ich spoločenské prijatie, skvalitňovať výrobky, procesy a obchodné modely a pomôcť európskym výrobcom k zefektívneniu.

Okrem zvýšenia produktivity a efektívnosti umelá inteligencia sľubuje umožniť ľuďom, aby dosiahli zatiaľ nedosiahnutú inteligenciu, otvára dvere novým objavom a pomáha riešiť niektoré z najväčších výziev sveta: od liečby chronických ochorení, predvídania ohnisk chorôb alebo znižovania úmrtnosti v dopravných nehodách, až po boj proti zmene klímy alebo predvídanie kybernetických hrozieb.

Tieto technológie môžu priniesť mnohé výhody zlepšením bezpečnosti výrobkov, ktoré budú menej náchylné na určité riziká. Napríklad prepojené a automatizované vozidlá by mohli

⁶ SWD(2018) 161 final.

⁷ Smernica 2006/42/ES

⁸ Sieť pre bezpečnosť spotrebiteľov zriadená smernicou 2001/95/ES o všeobecnej bezpečnosti výrobkov (GPSD), smernicou 2006/42/ES o strojových zariadeniach a smernicou 2014/53/EÚ o rádiových zariadeniach – expertné skupiny zložené z členských štátov, priemyslu a iných zainteresovaných strán, napríklad združenie spotrebiteľov.

⁹ COM(2018) 246 final.

¹⁰ Smernica 85/374/EHS

¹¹ Expertná skupina pre zodpovednosť a nové technológie bola vytvorená s cieľom poskytnúť Komisii odborné znalosti o uplatniteľnosti smernice o zodpovednosti za výrobky a vnútroštátnych predpisov o občianskoprávnej zodpovednosti, ako aj pomoc pri vypracúvaní smerodajných zásad v prípade úpravy uplatniteľných právnych predpisov súvisiacich s novými technológiami. Pozostáva z dvoch formácií, a to z „formácie pre zodpovednosť za výrobky“ a „formácie pre nové technológie“, pozri <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1>.

Správu „formácie pre nové technológie“ o zodpovednosti za umelú inteligenciu a ďalšie nové digitálne technológie pozri na adrese https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

zlepšiť bezpečnosť cestnej premávky, keďže väčšina dopravných nehôd je v súčasnosti spôsobená ľudským zavinením¹². Navyše systémy internetu vecí sú navrhnuté tak, aby prijímali a spracúvali obrovské množstvá údajov z rôznych zdrojov. Túto zvýšenú úroveň informácií možno použiť tak, aby sa výrobky mohli samé prispôbiť a následne sa stali bezpečnejšími. Nové technológie môžu zefektívniť sťahovanie výrobkov z obehu, keďže používatelia by napríklad mohli byť varovaní pred bezpečnostným problémom cez výrobky¹³. Ak sa pri používaní pripojeného výrobku vyskytne bezpečnostný problém, výrobcovia môžu priamo komunikovať s používateľmi, a to s cieľom na jednej strane varovať používateľov pred rizikami a na druhej strane priamo problém vyriešiť, ak je to možné, napríklad tým, že poskytnú bezpečnostnú aktualizáciu. Napríklad v roku 2017 istý výrobca smartfónov sťahoval jedno zo svojich zariadení a aby používatelia prestali nebezpečné zariadenia používať, vykonal aktualizáciu softvéru, ktorá znížila kapacitu batérie mobilných telefónov na nulu¹⁴.

Nové technológie môžu navyše prispieť k zlepšeniu vysledovateľnosti výrobkov. Napríklad niektoré prepájacie funkcie internetu vecí umožnia podnikom a orgánom dohľadu nad trhom sledovať nebezpečné výrobky a identifikovať riziká v rôznych dodávateľských reťazcoch¹⁵.

Umelá inteligencia, internet vecí a robotika môžu priniesť hospodárstvu a spoločnosti príležitosti, ale takisto môžu ohroziť zákonom chránené majetkové aj nemajetkové záujmy. Čím viac sa pole ich pôsobnosti rozšíri, tým vyššie bude riziko výskytu takejto ujmy. V tejto súvislosti je nevyhnutné preskúmať, či a do akej miery je súčasný právny rámec bezpečnosti a zodpovednosti stále vhodný na ochranu používateľov.

2. Bezpečnosť

V oznámení Komisie „Budovanie dôvery v umelú inteligenciu sústredenú na človeka“ sa uvádza, že *systémy umelej inteligencie by mali mať integrované mechanizmy bezpečnosti a mechanizmy špecificky navrhutej ochrany údajov, aby sa zabezpečilo, že sú v každom kroku preukázateľne bezpečné, pričom sa zohľadní fyzická a duševná bezpečnosť všetkých zainteresovaných*¹⁶.

V tejto časti sa pri posudzovaní právnych predpisov Únie v oblasti bezpečnosti výrobkov skúma, či súčasný legislatívny rámec Únie obsahuje príslušné prvky, ktorými sa zabezpečí integrácia bezpečnosti do nových technológií, najmä systémov umelej inteligencie, a to už v štádiu návrhu.

¹² Odhaduje sa, že približne 90 % dopravných nehôd je spôsobených ľudským zavinením. Pozri správu Komisie s názvom Záchrana životov: Posilnenie bezpečnosti automobilov v EÚ [COM(2016) 0787 final].

¹³ Napríklad vodič auta môže byť v prípade nehody upozornený, aby spomalil.

¹⁴ OECD (2018), „Meranie a maximalizácia globálneho vplyvu sťahovania výrobkov: správa z workshopu OECD, *OECD Science, Technology and Industry Policy Papers*, č. 56, OECD Publishing, Paríž, <https://doi.org/10.1787/ab757416-en>.

¹⁵ OECD (2018), „Zefektívnenie globálneho sťahovania výrobkov z obehu: podkladová správa OECD“, *OECD Science, Technology and Industry Policy Papers*, č. 58, OECD Publishing, Paríž, <https://doi.org/10.1787/ef71935c-en>.

¹⁶ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Budovanie dôvery v umelú inteligenciu sústredenú na človeka, Brusel, 8.4.2019 COM(2019) 168 final.

Táto správa sa zameriava predovšetkým na smernicu o všeobecnej bezpečnosti výrobkov¹⁷ a na harmonizované právne predpisy v oblasti výrobkov, ktoré sa riadia horizontálnymi pravidlami „nového prístupu“¹⁸ a/alebo „nového legislatívneho rámca“ (ďalej len „právne predpisy alebo rámec Únie v oblasti bezpečnosti výrobkov“)¹⁹. Horizontálne pravidlá zabezpečujú vzájomný súlad odvetvových pravidiel v oblasti bezpečnosti výrobkov.

Cieľom právnych predpisov Únie v oblasti bezpečnosti výrobkov je zabezpečiť, aby výrobky uvedené na trh Únie spĺňali vysoké zdravotné, bezpečnostné a environmentálne požiadavky a aby sa takéto výrobky mohli v rámci Únie voľne pohybovať. Odvetvové právne predpisy²⁰ dopĺňa smernica o všeobecnej bezpečnosti výrobkov²¹, ktorá vyžaduje, aby boli bezpečné všetky spotrebné výrobky, a to aj keď nie sú upravené v odvetvových právnych predpisoch EÚ. Pravidlá bezpečnosti dopĺňa trhový dohľad a právomoci, ktoré vnútroštátnym orgánom vyplývajú z nariadenia o dohľade nad trhom²² a zo smernice o všeobecnej bezpečnosti výrobkov²³. V oblasti dopravy sa ďalšie pravidlá Únie a členských štátov vzťahujú na uvádzanie motorových vozidiel²⁴, lietadiel alebo lodí do prevádzky. Jasné pravidlá platia v oblasti bezpečnosti počas prevádzky, a to aj pokiaľ ide o úlohy operátorov a dohľad zo strany orgánov.

Základným prvkom právnych predpisov Únie v oblasti bezpečnosti výrobkov je aj európska normalizácia. Vzhľadom na globálny charakter digitalizácie a nových digitálnych technológií má medzinárodná spolupráca v oblasti normalizácie osobitný význam pre konkurencieschopnosť európskeho priemyslu.

Značná časť rámca Únie v oblasti bezpečnosti výrobkov vznikla pred príchodom digitálnych technológií, ako sú umelá inteligencia, internet vecí či robotika. Preto nie vždy obsahuje ustanovenia, ktoré by výslovne riešili nové výzvy a riziká spojené s týmito novými technológiami. Hoci je súčasný rámec bezpečnosti výrobkov technologicky neutrálny, neznamená to, že by sa na výrobky vybavené týmito technológiami nevzťahoval. Okrem toho v následných legislatívnych aktoch, ktoré tvoria súčasť tohto rámca, napríklad v odvetví zdravotníckych pomôcok alebo automobilov, sa už niektoré aspekty nových digitálnych technológií zohľadnili, napríklad automatizované rozhodnutia, softvér ako samostatný výrobok a prepojitelnosť.

¹⁷ Smernica Európskeho parlamentu a Rady 2001/95/ES z 3. decembra 2001 o všeobecnej bezpečnosti výrobkov (Ú. v. ES L 11, 15.1.2002, s. 4 – 17).

¹⁸ Ú. v. ES C 136, 4.6.1985, s. 1.

¹⁹ Nariadenie (ES) č. 2008/765 a rozhodnutie (ES) č. 2008/768

²⁰ Táto schéma sa nevzťahuje na právne predpisy Únie v oblasti dopravy a automobilov.

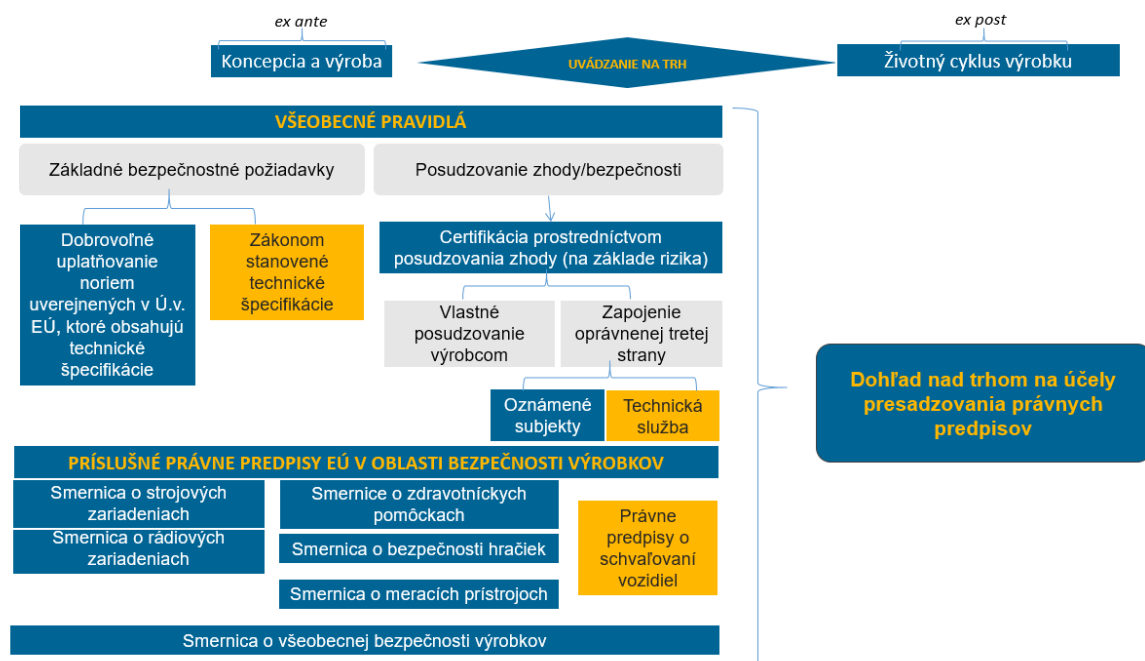
²¹ Smernica Európskeho parlamentu a Rady 2001/95/ES z 3. decembra 2001 o všeobecnej bezpečnosti výrobkov (Ú. v. ES L 11, 15. 1. 2002, s. 4 – 17).

²² Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93, Ú. v. EÚ L 218, 13.8.2008, s. 30 – 47, ELI: <http://data.europa.eu/eli/reg/2008/765/oj>, a od roku 2021 nariadenie Európskeho parlamentu a Rady (EÚ) 2019/1020 z 20. júna 2019 o dohľade nad trhom a súlade výrobkov a o zmene smernice 2004/42/ES a nariadení (ES) č. 765/2008 a (EÚ) č. 305/2011, Ú. v. EÚ L 169, 25.6.2019, s. 1 – 44, ELI: <http://data.europa.eu/eli/reg/2019/1020/oj>

²³ Článok 8 ods. 1 písm. b) bod 3) smernice o všeobecnej bezpečnosti výrobkov.

²⁴ Napríklad smernica 2007/46/ES – typové schválenie motorových vozidiel a ich prípojných vozidiel, systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá, a nariadenie Európskeho parlamentu a Rady (EÚ) 2018/858 z 30. mája 2018 o schvaľovaní motorových vozidiel a ich prípojných vozidiel, ako aj systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá a o dohľade nad trhom s nimi, ktorým sa menia nariadenia (ES) č. 715/2007 a (ES) č. 595/2009 a zrušuje smernica 2007/46/ES.

Základná logika súčasných právnych predpisov Únie v oblasti bezpečnosti výrobkov²⁵



Predstavujeme tu výzvy, ktoré vplývajú na rámec Únie pre bezpečnosť výrobkov v súvislosti s príchodom nových technológií.

Základnou vlastnosťou čoraz väčšieho počtu výrobkov a služieb je **prepojitelnosť**. Táto vlastnosť spochybňuje tradičnú koncepciu bezpečnosti, keďže prepojitelnosť môže priamo ohroziť bezpečnosť výrobku a v prípade hackerského útoku môže nepriamo vyvolať bezpečnostnú hrozbu a ovplyvniť bezpečnosť používateľov.

Príkladom je oznámenie týkajúce sa inteligentných hodín pre deti²⁶, ktoré poslal Island cez systém včasného varovania EÚ. Tento výrobok by dieťaťu, ktoré ho nosí, nespôsobil priamu škodu, ale keďže nie je ani minimálne zabezpečený, možno ho ľahko použiť na získanie prístupu k dieťaťu. Vzhľadom na to, že jedným zo zamýšľaných účelov tohto výrobku je chrániť bezpečnosť detí pomocou lokalizácie, spotrebiteľ očakáva, že výrobok neohrozí bezpečnosť detí tým, že umožní, aby ich ktokoľvek sledoval či kontaktoval.

Ďalší príklad sa uvádza v oznámení Nemecka týkajúcom sa osobného automobilu²⁷. Rádio vo vozidle môže mať určité medzery v zabezpečení softvéru, ktoré umožňujú neoprávnený prístup tretej strany do prepojených ovládacích systémov vo vozidle. Ak by tieto nedostatky v zabezpečení softvéru využila tretia strana na nekalé účely, mohlo by dôjsť k dopravnej nehode.

Kybernetickým hrozbám môžu byť vystavené aj priemyselné aplikácie, ktoré môžu v prípade nedostatočnej úrovne zabezpečenia ovplyvniť bezpečnosť väčšieho počtu ľudí. Môže k tomu dôjsť napríklad v prípade kybernetického útoku na systém ovládania kritických bodov v priemyselnom závode s cieľom vyvolať výbuch, ktorý môže priniesť straty na životoch.

²⁵ Tento opis nezahŕňa požiadavky na právne predpisy týkajúce sa životného cyklu výrobku, t. j. používania a údržby, a uvádza sa len na účel ilustrácie.

²⁶ Oznámenie Islandu cez RAPEX uverejnené na webovom sídle EÚ Safety Gate (A12/0157/19)

²⁷ Oznámenie Nemecka cez RAPEX uverejnené na webovom sídle EÚ Safety Gate (A12/1671/15)

V právnych predpisoch Únie v oblasti bezpečnosti výrobkov sa väčšinou nestanovujú konkrétne povinné základné požiadavky vo vzťahu k počítačovým hrozbám, ktoré majú vplyv na bezpečnosť používateľov. Ustanovenia týkajúce sa bezpečnostných aspektov sa však nachádzajú v nariadení o zdravotníckych pomôckach²⁸, smernici o meracích prístrojoch²⁹, smernici o rádiových zariadeniach³⁰ či právnych predpisoch o typovom schvaľovaní vozidiel³¹. V akte o kybernetickej bezpečnosti³² sa zavádza rámec dobrovoľnej certifikácie kybernetickej bezpečnosti pre výrobky, služby a procesy informačných a komunikačných technológií (IKT) a v právnych predpisoch Únie v oblasti bezpečnosti výrobkov sa stanovujú povinné požiadavky.

Okrem toho bezpečnostné riziko môže predstavovať aj strata prepojitelnosti nových digitálnych technológií. Ak napríklad poplašné požiarne zariadenie stratí prepojitelnosť, môže sa stať, že v prípade požiaru používateľa neupozorní.

V súčasných právnych predpisoch Únie v oblasti bezpečnosti výrobkov je bezpečnosť cieľom verejnej politiky. Koncepcia bezpečnosti sa viaže na používanie výrobku a riziká, napríklad mechanické či elektrické, ktoré treba riešiť, aby bol výrobok bezpečný. Treba poznamenať, že podľa toho, o ktorý právny predpis Únie v oblasti bezpečnosti výrobkov ide, sa používanie výrobku vzťahuje nielen na zamýšľané, ale aj predpokladané použitie, a v niektorých prípadoch, ako napríklad v smernici o strojových zariadeniach³³ aj na racionálne predpokladané nesprávne použitie.

Koncepcia bezpečnosti v súčasných právnych predpisoch Únie v oblasti bezpečnosti výrobkov je v súlade s rozšírenou koncepciou bezpečnosti, ktorej cieľom je chrániť spotrebiteľov a používateľov. Koncepcia bezpečnosti výrobkov zahŕňa ochranu pred všetkými druhmi rizík vyplývajúcich z výrobku vrátane nielen mechanických, chemických a elektrických rizík, ale aj kybernetických rizík a rizík súvisiacich so stratou prepojitelnosti zariadení.

V tejto súvislosti by sa mohlo zvažovať, aby sa do rozsahu pôsobnosti príslušných právnych predpisov Únie začlenili výslovné ustanovenia, ktoré by zabezpečili lepšiu ochranu používateľov a väčšiu právnu istotu.

Jednou z hlavných vlastností umelej inteligencie je jej **autonómnosť**³⁴. Umelá inteligencia môže mať nezamýšľaný vplyv, ktorý by mohol používateľov a vystavené osoby poškodiť.

V miere, do akej môžu výrobcovia vopred určiť budúce „správanie“ výrobkov vybavených umelou inteligenciou na základe posúdenia rizika pred uvedením výrobkov na trh, už dnes rámec Únie v oblasti bezpečnosti výrobkov ukladá výrobcom povinnosti zohľadňovať

²⁸ Nariadenie (EÚ) 2017/745 o zdravotníckych pomôckach

²⁹ Smernica 2014/32/EÚ o sprístupňovaní meradiel na trhu

³⁰ Smernica 2014/53/EÚ o rádiových zariadeniach

³¹ Smernica 2007/46/ES – typové schválenie motorových vozidiel a ich prípojných vozidiel, systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá Smernica bude zrušená a nahradená nariadením (EÚ) 2018/858 o schvaľovaní motorových vozidiel a ich prípojných vozidiel, ako aj systémov, komponentov a samostatných technických jednotiek určených pre takéto vozidlá a o dohľade nad trhom s nimi, ktorým sa menia nariadenia (ES) č. 715/2007 a (ES) č. 595/2009 a zrušuje smernica 2007/46/ES s účinnosťou od 1. septembra 2020.

³² Nariadenie (EÚ) 2019/881

³³ Smernica 2006/42/ES o strojových zariadeniach

³⁴ Hoci výrobky vybavené umelou inteligenciou vedú autonómne konať na základe vnímania svojho prostredia a bez toho, aby postupovali podľa vopred stanoveného súboru pokynov, ich správanie sa riadi len stanoveným cieľom a ďalšími koncepčnými možnosťami, ktoré zvolili vývojári. „

v posúdení rizika „používanie“³⁵ výrobkov v celom životnom cykle. Predpokladá sa v ňom aj to, že výrobcovia musia používateľom poskytovať pokyny a bezpečnostné informácie alebo výstrahy³⁶. V tejto súvislosti sa napríklad v smernici o rádiových zariadeniach³⁷ od výrobcu vyžaduje, aby priložil pokyny s informáciami o tom, ako používať rádiové zariadenie v súlade s jeho zamýšľaným účelom.

V budúcnosti sa môžu vyskytnúť aj situácie, keď výsledky práce systémov umelej inteligencie nebude možné určiť v plnej miere vopred. V takýchto situáciách sa už v posúdení rizika, ktoré sa uskutočnilo pred uvedením výrobku na trh, nemusí reálne odrážať používanie, fungovanie či správanie výrobku. Ak v týchto prípadoch dôjde v dôsledku autonómneho správania k zmene³⁸ zamýšľaného účelu, ktorý výrobca pôvodne predpokladal, a negatívne sa to odrazí na dodržiavaní bezpečnostných požiadaviek, môže sa požadovať, aby sa posúdenie samoučiaceho výrobku vykonalo nanovo³⁹.

Podľa súčasného rámca sa už teraz požaduje, aby výrobcovia hneď, ako zistia, že výrobok v ľubovoľnom štádiu svojho životného cyklu predstavuje riziko s vplyvom na bezpečnosť, okamžite informovali príslušné orgány a prijali opatrenia, ktoré zabránia, aby boli používatelia vystavení riziku⁴⁰.

Popri posudzovaní rizika pred uvedením výrobku na trh by sa mohol zaviesť nový postup posudzovania rizika pre výrobky, ktoré prechádzajú počas životného cyklu dôležitými zmenami, napríklad výrobok získa funkciu, ktorú výrobca pri pôvodnom posudzovaní rizika nepredpokladal. Tento nový postup by sa mal zamerať na vplyv autonómneho správania na bezpečnosť v celom životnom cykle výrobku. Posúdenie rizika by mal uskutočniť príslušný hospodársky subjekt. Okrem toho by sa mohli v príslušných právnych predpisoch Únie posilniť požiadavky na výrobcov, pokiaľ ide o pokyny a varovania pre používateľov.

³⁵ V právnych predpisoch Únie v oblasti bezpečnosti výrobkov výrobcovia vykonávajú posúdenie rizika na základe zamýšľaného účelu výrobku, predpokladaného použitia a/alebo racionálne predpokladaného nesprávneho použitia výrobku.

³⁶ Rozhodnutie Európskeho parlamentu a Rady č. 768/2008/ES z 9. júla 2008 o spoločnom rámci na uvádzanie výrobkov na trh a o zrušení rozhodnutia 93/465/EHS, Ú. v. EÚ L 218, 13.8.2008, s. 82 – 128. V prílohe I, článku R2.7 sa uvádza: „*Výrobcovia zabezpečia, aby bol k výrobkom dodaný návod na použitie a bezpečnostné pokyny v jazyku, ktorý je ľahko zrozumiteľný spotrebiteľom a iným koncovým používateľom a ktorý určí dotknutý členský štát.*“

³⁷ V článku 10 ods. 8 sa odkazuje na pokyny pre koncového používateľa a v prílohe VI na vyhlásenie EÚ o zhode.

³⁸ V kontexte umeleckej inteligencie sa termín „samoučenie“ používa prevažne na označenie toho, že prístroje sú schopné učiť sa počas tréningu; zatiaľ sa nepožaduje, aby sa prístroje vybavené umelou inteligenciou učili aj po zavedení; naopak, najmä v zdravotníctve sa prístroje vybavené umelou inteligenciou po úspešne ukončenom tréningu väčšinou prestanú učiť. V tomto štádiu teda z autonómneho správania, ktoré prinášajú systémy umelej inteligencie, nevyplýva, že výrobok vykonáva úlohy, ktoré by vývojári neboli predpokladali.

³⁹ To je v súlade s oddielom 2.1 „Modrej príručky“ na vykonávanie právnych predpisov EÚ týkajúcich sa výrobkov z roku 2016.“

⁴⁰ Článok 5 smernice Európskeho parlamentu a Rady 2001/95/ES z 3. decembra 2001 o všeobecnej bezpečnosti výrobkov.

Podobné posudzovanie rizika sa už vyžaduje v právnych predpisoch týkajúcich sa dopravy⁴¹; napríklad v právnych predpisoch o železničnej doprave platí, že ak sa železničné vozidlo po certifikácii upraví, autor úpravy podlieha konkrétnemu postupu a na základe jasných kritérií sa určí, či treba alebo netreba zapojiť daný orgán.

Schopnosť produktov a systémov umelej inteligencie učiť sa môže znamenať, že prístroj prijme iné rozhodnutia, ako pôvodne zamýšľali výrobcovia, a teda ako očakávajú používatelia. To vyvoláva otázky v súvislosti s ovládaním človekom. Ľudia si budú môcť vybrať, ako a či na dosiahnutie človekom zvolených cieľov delegujú rozhodnutia na výrobky a systémy umelej inteligencie⁴². V súčasných právnych predpisoch Únie v oblasti bezpečnosti výrobkov sa ľudský dozor v kontexte samoučiacich výrobkov a systémov umelej inteligencie výslovne nerieši⁴³.

V príslušných právnych predpisoch Únie možno na ochranu stanoviť osobitné požiadavky na ľudský dohľad od návrhu výrobku a počas celého životného cyklu výrobkov a systémov umelej inteligencie.

Budúce „správanie“ aplikácií umelej inteligencie by mohlo priniesť **riziká pre duševné zdravie**⁴⁴ používateľov vyvolané napríklad spoluprácou s humanoidnými robotmi a systémami umelej inteligencie, a to v domácom aj pracovnom prostredí. V tejto súvislosti sa dnes pojem bezpečnosť všeobecne používa na označenie vnímanej hrozby fyzického poškodenia, ktoré môže používateľovi priniesť nová digitálna technológia. Zároveň v právnom rámci EÚ sú bezpečné výrobky vymedzené ako výrobky, ktoré nepredstavujú žiadne riziko alebo len minimálne riziká pre bezpečnosť a zdravie osôb. Panuje zhoda v tom, že vymedzenie pojmu zdravie zahŕňa fyzickú aj duševnú pohodu. No koncepcia bezpečnosti výrobkov by mala v legislatívnom rámci výslovne pokrývať riziká pre duševné zdravie.

Napríklad autonómnosť by nemala spôsobovať dlhšie obdobia nadmerného stresu a nepohodlia, ani poškodzovať duševné zdravie. V tomto ohľade sa za faktory, ktoré pozitívne ovplyvňujú pocit bezpečia u starších ľudí⁴⁵, považujú: bezpečné vzťahy s personálom služieb zdravotnej starostlivosti, kontrola nad denným režimom a informovanosť o ňom. Výrobcovia robotov, ktorí komunikujú so staršími ľuďmi, by mali tieto faktory zohľadniť, aby predišli ohrozeniu duševného zdravia.

⁴¹ V prípade akejkoľvek zmeny železničného systému, ktorá by mohla mať vplyv na bezpečnosť (napr. technická, prevádzková alebo aj organizačná zmena, ktorá by mohla zasiahnuť do prevádzky alebo údržby), sa uplatňuje postup opísaný v prílohe I k vykonávaciemu nariadeniu Komisie (EÚ) 2015/1136 (Ú. v. EÚ L 185, 14.7.2015, s. 6).

V prípade „zásadnej zmeny“ by mal nezávislý „posudzovací orgán“ (môže ísť o vnútroštátny bezpečnostný alebo iný odborne príslušný orgán) predložiť navrhovateľovi zmeny správu o posúdení bezpečnosti.

V procese analýzy rizík uplatní navrhovateľ zmeny primerané opatrenia na zmiernenie rizík (ak je navrhovateľom železničný alebo infraštruktúrny podnik, uplatňovanie nariadenia je súčasťou jeho systému riadenia bezpečnosti, na ktorý dohliada vnútroštátny bezpečnostný orgán).

⁴² Politické a investičné odporúčania pre dôveryhodnú umelú inteligenciu, expertná skupina na vysokej úrovni pre umelú inteligenciu, jún 2019.

⁴³ Tým sa však nevylučuje, že dohľad môže byť v danej situácii potrebný vzhľadom na niektoré zo súčasných všeobecnejších povinností týkajúcich sa uvedenia výrobku na trh.

⁴⁴ Ústava Svetovej zdravotníckej organizácie (WHO), prvá záležitosť: „Zdravie je stav úplnej fyzickej, duševnej a spoločenskej pohody a nie len stav bez choroby alebo invalidity.“ (<https://www.who.int/about/who-we-are/constitution>)

⁴⁵ Spoločenské roboty: Technologické, spoločenské a etické aspekty interakcie človeka a robota, s. 237 – 264, výskum, Neziha Akalin, Annica Kristoffersson a Amy Loutfi, júl 2019.

Z hľadiska pôsobnosti príslušných právnych predpisov EÚ by sa mohlo pre výrobcov okrem iného humanoidných robotov vybavených umelou inteligenciou zväžiť zavedenie výslovnej povinnosti, aby zohľadňovali nemajetkovú ujmu, ktorú by ich výrobky mohli spôsobiť používateľom, najmä zraniteľným používateľom, ako sú staršie osoby v prostredí zdravotnej starostlivosti.

Ďalšou podstatnou vlastnosťou výrobkov a systémov založených na umelej inteligencii je **závislosť od údajov**. Aby systémy a výrobky založené na umelej inteligencii prijímali rozhodnutia tak, ako to zamýšľal výrobca, musia mať presné a relevantné údaje.

Právne predpisy Únie v oblasti bezpečnosti výrobkov sa výslovne nezameriavajú na bezpečnostné riziká, ktoré vyvolávajú nesprávne údaje. Výrobcovia by však mali v štádiu návrhu a testovania výrobku podľa jeho „použitia“ predpokladať presnosť údajov a ich relevantnosť pre bezpečnostné funkcie.

Napríklad systém založený na umelej inteligencii, ktorý je určený na odhaľovanie špecifických predmetov, môže mať ťažkosti pri rozpoznávaní položiek v zlých podmienkach osvetlenia, takže jeho projektanti by mali zahrnúť údaje pochádzajúce zo skúšok výrobkov v typických aj slabo osvetlených prostrediach.

Ďalší príklad sa týka poľnohospodárskych robotov, ako sú napríklad roboty na zber ovocia, ktoré sa zameriavajú na zisťovanie a lokalizáciu zrelých plodov na stromoch alebo na zemi. Zatiaľ čo príslušné algoritmy už vykazujú viac ako 90-percentnú mieru úspešnosti klasifikácie, zlyhanie v súboroch údajov, ktoré zásobujú tieto algoritmy, môže tieto roboty priviesť k zlému rozhodnutiu a v dôsledku toho sa môže zranieť osoba alebo zviera.

Vzniká otázka, či by právne predpisy Únie v oblasti bezpečnosti výrobkov mali obsahovať osobitné požiadavky, ktorými by sa riešili riziká spojené s chybami v údajoch v štádiu návrhu, ako aj mechanizmy, ktoré zabezpečia, že kvalita údajov sa zachová v celom cykle používania výrobkov a systémov umelej inteligencie.

Ďalšou významnou vlastnosťou niektorých výrobkov a systémov založených na umelej inteligencii je **nepriehľadnosť**, ktorú môže spôsobiť ich schopnosť zlepšovať výkon na základe poučenia zo skúsenosti. Výrobky a systémy založené na umelej inteligencii možno v závislosti od metodického prístupu charakterizovať rôznymi stupňami nepriehľadnosti. To môže spôsobiť, že rozhodovací postup systému je náročné vysledovať („efekt čiernej skrinky“). Pre ľudí nemusí byť potrebné rozumieť každému kroku rozhodovacieho postupu, ale čím sú algoritmy umelej inteligencie vyspelejšie a prenikajú do kritických odvetví, ľudia by rozhodne mali rozumieť tomu, ako systém dospel k algoritmickému rozhodnutiu. To by bolo zvlášť dôležité pre následný mechanizmus presadzovania práva, keďže to umožní orgánom presadzovania práva vysledovať zodpovednosť za správanie a rozhodnutia systémov umelej inteligencie. Uznáva sa to aj v oznámení Komisie o budovaní dôvery v umelú inteligenciu sústredenú na človeka⁴⁶.

V právnych predpisoch Únie v oblasti bezpečnosti výrobkov sa narastajúce riziká vyplývajúce z nepriehľadnosti systémov založených na algoritmoch výslovne neriešia. Preto treba zväžiť požiadavky na transparentnosť algoritmov, ako aj na spoľahlivosť, zodpovednosť a v prípade potreby ľudské ovládanie a nezaujatosť výsledkov⁴⁷, ktoré sú

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

⁴⁷ Podľa kľúčových požiadaviek, ako ich navrhla expertná skupina na vysokej úrovni v Etických usmerneniach pre dôveryhodnú umelú inteligenciu: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>

zvlášť dôležité pre následný mechanizmus presadzovania práva a budovanie dôvery používateľov v tieto technológie. Túto výzvu by sa dalo vyriešiť uložením požiadavky na vývojárov algoritmov, aby v prípade porúch odtajnil parametre návrhu a metadáta údajových súborov.

K ďalším rizikám, ktoré môžu ovplyvniť bezpečnosť, patria riziká vyplývajúce zo **zložitosti výrobkov a systémov** vzhľadom na to, že rôzne komponenty, zariadenia a výrobky sa môžu integrovať a vzájomne ovplyvňovať svoje fungovanie (napr. výrobky, ktoré sú súčasťou inteligentného domáceho ekosystému).

Touto zložitou sa už zaoberá právny rámec Únie v oblasti bezpečnosti, na ktorý sa odkazuje na začiatku tohto oddielu⁴⁸. Hlavne vtedy, keď výrobca vykonáva v súvislosti s výrobkom posúdenie rizika, musí zväžiť zamýšľané použitie, predvídateľné použitie a prípadne aj racionálne predpokladané nesprávne použitie.

Ak v tejto súvislosti **výrobca predpokladá, že jeho zariadenie bude prepojené s ďalšími zariadeniami a bude s nimi komunikovať, malo by sa to pri posúdení rizika vziať do úvahy**. Použitie, resp. nesprávne použitie sa stanovuje napríklad na základe skúseností s používaním rovnakého typu výrobku v minulosti, vyšetrovania porúch alebo ľudského správania.

Zložitost' systémov sa konkrétnejšie rieši aj v odvetvových právnych predpisoch v oblasti bezpečnosti, ako je nariadenie o zdravotníckych pomôckach, a do určitej miery v právnych predpisoch o všeobecnej bezpečnosti výrobkov⁴⁹. Napríklad výrobca prepojeného zariadenia, ktoré má byť súčasťou inteligentného domáceho ekosystému, by mal byť schopný racionálne predpokladať, že jeho výrobky budú mať vplyv na bezpečnosť iných výrobkov.

Túto zložitost' riešia na systémovej úrovni aj právne predpisy v oblasti dopravy. V prípade vozidiel, vlakov a lietadiel sa typové schvaľovanie a osvedčovanie uskutočňuje tak pre každý komponent, ako aj pre celé vozidlo alebo lietadlo. Súčasťou posudzovania bezpečnosti sú technický stav vozidla, letová spôsobilosť a interoperabilita železníc. V oblasti dopravy musí „systémy“ „povoliť“ príslušný orgán buď na základe posúdenia zhody s jasnými technickými požiadavkami, ktorú vykonala tretia strana, alebo po preukázaní toho, ako sa vyriešili riziká. V riešení sa prevažne spája úroveň „výrobok“ a úroveň „systém“.

Právne predpisy Únie o bezpečnosti výrobkov vrátane právnych predpisov v oblasti dopravy už do istej miery zohľadňujú zložitost' výrobkov či systémov v snahe riešiť riziká, ktoré by mohli mať vplyv na bezpečnosť používateľov.

Zložité systémy často zahŕňajú **softvér**, ktorý je základným komponentom systému založeného na umelej inteligencii. Vo všeobecnosti má výrobca konečného výrobku povinnosť predvídať v rámci počiatočného posúdenia riziká softvéru, ktorý je integrovaný do daného výrobku v čase jeho uvedenia na trh.

Niektoré právne predpisy Únie v oblasti bezpečnosti výrobkov výslovne odkazujú na softvér integrovaný do výrobku. Napríklad v smernici o strojových zariadeniach⁵⁰ sa vyžaduje, že chyba softvéru v ovládacom systéme nesmie viesť k nebezpečným situáciám.

⁴⁸ Nariadenie (ES) 2008/765 a rozhodnutie (ES) 2008/768 a harmonizované odvetvové právne predpisy v oblasti bezpečnosti výrobkov, napr. smernica 2006/42/ES o strojových zariadeniach.

⁴⁹ V článku 2 smernice o všeobecnej bezpečnosti výrobkov sa uvádza, že bezpečný výrobok zohľadňuje „vplyv na iné výrobky, ak sa racionálne predpokladá, že sa bude používať s inými výrobkami“.

⁵⁰ Oddiel 1.2.1 prílohy I k smernici o strojových zariadeniach.

V právnych predpisoch Únie v oblasti bezpečnosti výrobkov by sa aktualizácie softvéru dali porovnať s vykonávaním údržby z bezpečnostných dôvodov za predpokladu, že výrazne neupravujú výrobok, ktorý už bol uvedený na trh, a že neprinášajú nové riziká, s ktorými sa pri počiatočnom posúdení rizika nepočítalo. Ak sa však aktualizáciou softvéru podstatne upravuje výrobok, do ktorého sa softvér sťahuje, celý výrobok sa môže považovať za nový výrobok a v čase vykonania úpravy sa musí prehodnotiť súlad s príslušnými právnymi predpismi v oblasti bezpečnosti výrobkov⁵¹.

Odvetvové harmonizované právne predpisy Únie v oblasti bezpečnosti výrobkov neobsahujú vo všeobecnosti žiadne osobitné ustanovenia týkajúce sa samostatného softvéru, ktorý sa uvádza na trh ako taký alebo sa nahrá po uvedení výrobku na trh. Niektoré právne predpisy Únie sa však venujú samostatným softvérom, napríklad nariadenie o zdravotníckych pomôckach. Samostatný softvér nahratý do prepojených výrobkov, ktoré komunikujú prostredníctvom určitých rádiových modulov⁵², môže byť navyše regulovaný aj smernicou o rádiových zariadeniach prostredníctvom delegovaných aktov. V uvedenej smernici sa vyžaduje, aby špecifické triedy alebo kategórie rádiového zariadenia podporovali funkcie, ktoré zabezpečujú, aby sa nahratím softvéru neohrozil súlad tohto zariadenia⁵³.

V právnych predpisoch Únie v oblasti bezpečnosti výrobkov sa síce zohľadňujú bezpečnostné riziká vyplývajúce zo softvéru, ktorý je integrovaný do výrobku v čase jeho uvedenia na trh, ako aj z prípadných následných aktualizácií predvídaných výrobcom, no napriek tomu bude možno potrebné stanoviť osobitné a/alebo výslovné požiadavky na samostatný softvér (napr. „apka“, ktorá by sa sťahovala). Osobitná pozornosť by sa mala venovať samostatnému softvéru, ktorý výrobkom a systémom umelej inteligencie poskytuje bezpečnostné funkcie.

Možno bude potrebné stanoviť dodatočné povinnosti pre výrobcov s cieľom zabezpečiť, aby poskytovali funkcie, ktorými sa zabráni nahratiu softvéru, ktorý by mal vplyv na bezpečnosť počas životnosti výrobkov umelej inteligencie.

Na nové digitálne technológie majú v konečnom dôsledku vplyv aj **zložité hodnotové reťazce**. Táto zložitosť však nie je novinkou a nejde ani o problém, ktorý by bol výlučne spojený s novými digitálnymi technológiami, ako je umelá inteligencia alebo internet vecí. Je to tak napríklad aj v prípade výrobkov, ako sú počítače, servisné roboty alebo dopravné systémy.

Podľa rámca Únie upravujúceho bezpečnosť výrobkov nesie za bezpečnosť výrobku zodpovednosť výrobca, ktorý uvádza výrobok na trh, a to bez ohľadu na zložitosť hodnotového reťazca. Výrobcovia sú zodpovední za bezpečnosť konečného výrobku vrátane súčastí, ktoré sú do výrobku integrované, ako je napríklad softvér v počítači.

Niektoré právne predpisy Únie v oblasti bezpečnosti výrobkov už obsahujú ustanovenia, ktoré výslovne odkazujú na situácie, keď viaceré hospodárske subjekty zasahujú do daného výrobku pred jeho uvedením na trh. Napríklad v smernici o výtťahoch⁵⁴ sa vyžaduje, aby osoba zodpovedná za návrh a výrobu výtťahu poskytla osobe zodpovednej za inštalovanie a skúšanie výtťahu⁵⁵ „všetku potrebnú dokumentáciu a informácie s cieľom umožniť jej

⁵¹ [Modrá príručka na vykonávanie právnych predpisov EÚ týkajúcich sa výrobkov 2016](#).

⁵² Rádiové moduly sú elektronické zariadenia, ktoré vysielať a/alebo prijímajú rádiové signály (WIFI, Bluetooth) medzi dvoma zariadeniami.

⁵³ Článok 3 ods. 3 písm. i) smernice o rádiových zariadeniach.

⁵⁴ V súlade s článkom 16 ods. 2 smernice 2014/33/EÚ.

⁵⁵ V smernici 2014/33/EÚ o výtťahoch je inštalatér rovnocenný s výrobcom a musí prevziať zodpovednosť za návrh, výrobu, inštaláciu a uvedenie výtťahu na trh.

zabezpečenie správneho a bezpečného inštalovania a skúšania výťahu“. V smernici o strojových zariadeniach sa od výrobcov zariadení vyžaduje, aby prevádzkovateľovi poskytli informácie o tom, ako sa majú tieto zariadenia montovať spolu s iným strojovým zariadením⁵⁶.

Právne predpisy Únie v oblasti bezpečnosti výrobkov zohľadňujú zložitosť hodnotových reťazcov, pričom viacerým hospodárskym subjektom ukladajú povinnosti v súlade so zásadou „spoločnej zodpovednosti“.

Ukázalo sa, že v prípade súčasných zložitých hodnotových reťazcov je primerané, aby zodpovednosť za bezpečnosť konečného výrobku niesol výrobca. Avšak v hodnotových reťazcoch, ktoré by mohli byť dokonca ešte zložitejšie, by sa mohla právna istota zabezpečiť pomocou výslovných ustanovení požadujúcich, aby hospodárske subjekty v dodávateľskom reťazci a používatelia spolupracovali. Konkrétne každý aktér v hodnotovom reťazci, ktorý má vplyv na bezpečnosť výrobku (napr. výrobcovia softvéru), ako aj používatelia (ktorí napr. upravujú výrobok) by mali niesť zodpovednosť a poskytnúť ďalšiemu aktérovi v reťazci potrebné informácie a opatrenia.

3. Zodpovednosť

Ustanovenia v oblasti bezpečnosti výrobkov a zodpovednosti za výrobky sú dva komplementárne mechanizmy, ktorými sa na úrovni Únie sleduje ten istý politický cieľ – dosiahnuť fungujúci jednotný trh s tovarom, ktorý zaisťuje vysokú úroveň bezpečnosti, t. j. minimalizuje riziko poškodenia používateľov a poskytuje náhradu škody spôsobenej chybným tovarom.

Na úrovni jednotlivých členských štátov dopĺňajú tieto pravidlá Únie neharmonizované rámce občianskoprávnej zodpovednosti, ktoré zabezpečujú náhradu škody z rôznych príčin (ako výrobky a služby) a upravujú otázku zodpovednosti rôznych osôb (ako sú vlastníci, prevádzkovatelia alebo poskytovatelia služieb).

Optimalizácia bezpečnostných pravidiel Únie v oblasti umelej inteligencie síce môže pomôcť zabrániť nehodám, no nehody sa stávajú aj napriek tomu. Práve v takých prípadoch sa uplatňuje občianskoprávna zodpovednosť. Pravidlá občianskoprávnej zodpovednosti zohrávajú v našej spoločnosti dvojakú úlohu: na jednej strane zabezpečujú, aby sa odškodnili obeť, ktoré utrpeli škodu spôsobenú inými osobami, a na druhej strane ekonomicky motivujú zodpovednú stranu, aby takúto škodu nespôsobovala. Pravidlá zodpovednosti vždy musia hľadať rovnováhu medzi tým, aby chránili občanov pred poškodením, a zároveň umožňovali podnikom inovovať.

Rámce zodpovednosti v Únii fungujú dobre. Opierajú sa o paralelné uplatňovanie smernice o zodpovednosti za výrobky (smernica 85/374/EHS), ktorou sa harmonizovala zodpovednosť výrobcu chybných výrobkov, a iných neharmonizovaných vnútroštátnych režimov zodpovednosti.

Smernica o zodpovednosti za výrobky poskytuje úroveň ochrany, ktorú samotná subjektívna zodpovednosť na vnútroštátnej úrovni neposkytuje. Zavádza systém objektívnej

⁵⁶ V bode 1.7.4.2 prílohy I k smernici o strojových zariadeniach sa uvádza, že „Každá príručka s návodom na použitie musí podľa potreby obsahovať aspoň tieto informácie“ i) „návod na montáž, inštaláciu a zapojenie, vrátane výkresov, schém a upevňovacích prostriedkov, a označenie podvozku alebo inštalácie, na ktorý sa má strojové zariadenie namontovať“;

zodpovednosti výrobcu za škodu spôsobenú chybou v jeho výrobkoch. V prípade fyzickej alebo materiálnej škody má poškodená strana nárok na náhradu škody, ak preukáže škodu, chybu výrobku (t. j. že výrobok nezaručil bezpečnosť, ktorú verejnosť oprávnene očakáva) a príčinnú súvislosť medzi chybným výrobkom a škodou.

Vo vnútroštátnych neharmonizovaných režimoch sa stanovujú pravidlá subjektívnej zodpovednosti, podľa ktorých obeť, ktoré utrpeli škodu, úspešne uplatnia svoj nárok na náhradu škody, len ak preukážu zavinenie zodpovednou osobou, škodu a príčinnú súvislosť medzi zavinením a škodou. Zavádzajú sa v nich aj režimy objektívnej zodpovednosti, v rámci ktorých vnútroštátny zákonodarca pripisuje zodpovednosť za riziko určitej osobe bez toho, aby obeť musela dokázať zavinenie/chybu alebo príčinnú súvislosť medzi zavinením/chybou a škodou.

Vnútroštátne režimy zodpovednosti poskytujú obetiam, ktoré utrpeli škodu spôsobenú výrobkami a službami, viaceré súbežné nároky na náhradu škody, ktoré sú založené na subjektívnej alebo objektívnej zodpovednosti. Tieto nároky sú často namierené proti rôznym zodpovedným osobám a majú odlišné podmienky.

Napríklad obeť dopravnej nehody uplatňuje zvyčajne svoj nárok na náhradu škody voči vlastníkovi vozidla na základe jeho objektívnej zodpovednosti (t. j. voči osobe, ktorá uzavrela poistenie zodpovednosti za škodu spôsobenú prevádzkou motorového vozidla) a nárok na náhradu škody voči vodičovi na základe jeho subjektívnej zodpovednosti, pričom oba tieto nároky sa uplatňujú podľa vnútroštátneho občianskeho práva, ako aj nárok na náhradu škody voči výrobcovi podľa smernice o zodpovednosti za výrobky, ak bolo vozidlo chybné.

V súlade s harmonizovanými pravidlami upravujúcimi poistenie motorových vozidiel musí byť prevádzka vozidla poistená⁵⁷ a poisťovateľ je prakticky vždy prvým miestom, kde sa uplatňuje nárok na náhradu zdravotnej alebo majetkovej škody. V zmysle týchto pravidiel povinné poistenie odškodňuje obeť a chráni poistenú osobu, ktorá je podľa vnútroštátnych občianskoprávných predpisov⁵⁸ zodpovedná uhradiť finančné škody za nehodu spôsobenú prevádzkou motorového vozidla. Podľa smernice o zodpovednosti za výrobky výrobcovia nepodliehajú povinnému poisteniu. Pokiaľ ide o poistenie motorových vozidiel, s autonómnymi vozidlami sa v právnych predpisoch Únie nezaobchádza inak ako s neautonómnymi vozidlami. Tak ako na všetky vozidlá sa aj na tieto vozidlá musí vzťahovať poistenie zodpovednosti za škodu spôsobenú prevádzkou motorového vozidla, čo je pre poškodenú stranu najjednoduchší spôsob, ako získať odškodnenie.

Uzatvorením riadneho poistenia sa môžu zmierniť negatívne následky nehôd tak, že sa zabezpečí bezproblémové odškodnenie obeť. Jasné pravidlá zodpovednosti pomáhajú poisťovníam vypočítať svoje riziká a žiadať náhradu od strany, ktorá je v konečnom dôsledku zodpovedná za škodu. Ak napríklad dôjde k nehode spôsobenej chybou, poisťovateľ motorového vozidla môže po odškodnení obeť žiadať náhradu od výrobcu.

Vlastnosti nových digitálnych technológií, ako je umelá inteligencia, internet vecí a robotika, však spochybňujú aspekty rámcov zodpovednosti Únie a vnútroštátnych rámcov zodpovednosti a mohli by znížiť ich účinnosť. Niektoré z týchto vlastností by mohli sťažiť výsledovateľnosť škody spôsobenej ľudským správaním, v prípade ktorej by sa podľa

⁵⁷ V prípade motorových vozidiel sa harmonizácia vykonala smernicou 2009/103/ES o poistení zodpovednosti za škodu spôsobenú prevádzkou motorových vozidiel a o kontrole plnenia povinnosti poistenia tejto zodpovednosti.

⁵⁸ Vo väčšine členských štátov sa objektívna zodpovednosť uplatňuje na osobu, na ktorej meno je motorové vozidlo registrované.

vnútroštátnych pravidiel mohol uplatňovať nárok na náhradu škody na základe subjektívnej zodpovednosti. To znamená, že nároky na náhradu škody na základe vnútroštátnych zákonov o občianskoprávnej zodpovednosti možno iba ťažko dokázať, alebo je toto dokazovanie neprímerane nákladné, a preto obeť nemusí byť náležite odškodnená. Je dôležité, aby úroveň ochrany obetí nehôd spôsobených výrobkami a službami, medzi ktoré patria aj nové digitálne technológie ako umelá inteligencia, nebola nižšia v porovnaní s inými podobnými výrobkami a službami, v prípade ktorých by obeť získali náhradu škody na základe vnútroštátnych zákonov o občianskoprávnej zodpovednosti. Inak by to mohlo viesť k tomu, že spoločnosť tieto nové technológie neprijme úplne a bude mať váhavý postoj k ich používaniu.

Bude nutné posúdiť, či by výzvy, ktoré nové technológie predstavujú pre existujúce rámce, mohli spôsobiť aj právnu neistotu, pokiaľ ide o to, ako by sa mali uplatňovať existujúce právne predpisy (napr. ako by sa koncepcia zavinenia mohla uplatňovať na škody spôsobené umelou inteligenciou). To by následne mohlo odrádzať od investícií, ako aj zvyšovať náklady na informácie a poistenie výrobcov a iných podnikov v dodávateľskom reťazci, najmä európskych MSP. Ak by navyše členské štáty napokon riešili výzvy spojené s vnútroštátnymi rámcami zodpovednosti, viedlo by to k ďalšej fragmentácii, čím by sa zvýšili náklady na uvádzanie inovačných riešení umelej inteligencie na jednotný trh a obmedzilo by sa cezhraničné obchodovanie s týmito riešeniami. Je dôležité, aby si spoločnosti boli vedomé svojich rizík zodpovednosti v celom hodnotovom reťazci a mohli ich obmedziť alebo im predchádzať a účinne sa proti nim poistiť.

V tejto kapitole sa vysvetľuje, aké výzvy predstavujú nové technológie pre existujúce rámce a akým spôsobom by sa mohli tieto výzvy riešiť. Okrem toho osobitosti niektorých sektorov, akým je napríklad sektor zdravotnej starostlivosti, si môžu vyžadovať dodatočné posúdenie.

Zložitosť výrobkov, služieb a hodnotového reťazca: Technológie a priemysel prešli za posledné desaťročia výraznými zmenami. Najmä deliaca čiara medzi výrobkami a službami už nemusí byť taká jednoznačná ako v minulosti. Výrobky a poskytovanie služieb sú čoraz viac vzájomne prepojené. Zatiaľ čo zložité produkty a hodnotové reťazce nie sú pre európsky priemysel či jeho regulačný model ničím novým, softvér a rovnako aj umelá inteligencia si zasluhujú osobitnú pozornosť z hľadiska zodpovednosti za výrobky. Softvér zohráva zásadnú úlohu vo fungovaní veľkého množstva výrobkov a môže ovplyvniť ich bezpečnosť. Aby bolo možné použiť výrobok na to, na čo bol určený, je softvér integrovaný do výrobkov, ale sa môže dodávať aj samostatne. Počítač ani smartfón by sa bez softvéru nedali používať. To znamená, že softvér môže spôsobiť chybu v hmotnom výrobku a viesť k jeho fyzickému poškodeniu (pozri rámček o softvéri v časti o bezpečnosti). Výrobca výrobku by tak mohol byť v konečnom dôsledku zodpovedný v zmysle smernice o zodpovednosti za výrobky.

Avšak vzhľadom na to, že existujú rôzne typy a podoby softvérov, odpovedať na otázku klasifikácie softvéru ako služby alebo ako výrobku nemusí byť vždy jednoduché. Zatiaľ čo softvér riadiaci prevádzku hmotného výrobku by sa mohol považovať za súčasť alebo komponent tohto výrobku, klasifikovať niektoré formy samostatného softvéru by už mohlo byť ťažšie.

Hoci je vymedzenie výrobku podľa smernice o zodpovednosti za výrobky široké, jeho rozsah by sa mohol ešte viac objasniť, aby lepšie zohľadňoval zložitosť nových technológií a zabezpečoval, aby bolo za škody spôsobené výrobkami, ktoré sú chybné z dôvodu softvéru alebo iných digitálnych prvkov, vždy dostupné odškodnenie. Hospodárske subjekty, ako napríklad vývojári softvéru, by mohli vďaka tomu lepšie posúdiť, či by sa podľa smernice o zodpovednosti za výrobky mohli považovať za výrobcov.

Aplikácie umelej inteligencie tvoria často súčasť **zložitého prostredia internetu vecí**, v ktorom fungujú mnohé navzájom prepojené zariadenia a služby. Vzhľadom na kombináciu rôznych digitálnych komponentov v zložitom ekosystéme a rôznorodosť zúčastnených aktérov môže byť komplikované posúdiť, kde je pôvod potenciálnej škody a ktorá osoba za škodu nesie zodpovednosť. Vzhľadom na zložitosť týchto technológií môže byť pre obeť veľmi ťažké identifikovať zodpovednú osobu a dokázať všetky potrebné skutočnosti, aby mohli úspešne uplatniť svoj nárok na náhradu škody, ako sa vyžaduje podľa vnútroštátneho práva. Náklady na takúto expertízu môžu byť ekonomicky neúnosné a môžu odrádzať obeť od požadovania náhrady.

Okrem toho výrobky a služby, ktoré sa spoliehajú na umelú inteligenciu, budú v kontakte s tradičnými technológiami, čo povedie k ešte väčšej zložitosti aj v prípade zodpovednosti. Napríklad autonómne autá budú určitý čas jazdiť na cestách spolu s tradičnými autami. Podobne zložitá bude aj spolupôsobenie aktérov v niektorých odvetviach služieb (napríklad v oblasti riadenia dopravy a zdravotnej starostlivosti), kde budú rozhodovanie ľudí podporovať čiastočne automatizované systémy umelej inteligencie.

Podľa správy⁵⁹ formácie pre nové technológie v rámci expertnej skupiny pre zodpovednosť a nové technológie by sa mohli zvážiť úpravy vnútroštátnych právnych predpisov s cieľom uľahčiť dôkazné bremeno pre obeť škôd súvisiacich so umelou inteligenciou. Dôkazné bremeno by napríklad mohlo byť spojené s dodržiavaním zákonom stanovených osobitných povinností v oblasti kybernetickej bezpečnosti alebo iných bezpečnostných povinností (zo strany príslušného prevádzkovateľa): v prípade nedodržiavania týchto pravidiel by sa mohla uplatniť zmena dôkazného bremena, pokiaľ ide o zavinenie a príčinnú súvislosť.

Komisia skúma, či a do akej miery je potrebné obmedziť dôsledky zložitosti pomocou príslušnej iniciatívy EÚ, ktorá by zmiernila/zvrátila dôkazné bremeno požadované na základe vnútroštátnych pravidiel zodpovednosti za škody spôsobené prevádzkou aplikácií umelej inteligencie.

Pokiaľ ide o právne predpisy Únie, podľa smernice o zodpovednosti za výrobky by sa výrobok, ktorý nespĺňa povinné bezpečnostné predpisy, považoval za chybný bez ohľadu na zavinenie výrobcom. Môžu však existovať aj dôvody na to, aby sa zvážili spôsoby, ako podľa smernice uľahčiť dôkazné bremeno pre obeť: smernica sa opiera o vnútroštátne pravidlá týkajúce sa dôkazov a vzniku príčinnej súvislosti.

Prepojitelnosť a otvorenosť: V súčasnosti nie je celkom jasné, čo možno očakávať z hľadiska bezpečnosti, pokiaľ ide o škody vyplývajúce z narušenia kybernetickej bezpečnosti vo výrobku, a či by mohli byť takéto škody primerane nahradené podľa smernice o zodpovednosti za výrobky.

Nedostatky v oblasti kybernetickej bezpečnosti môžu existovať hneď od začiatku, keď sa výrobok uvedie do obehu, no môžu sa objaviť aj neskôr, dávno po tom, čo sa výrobok uviedol do obehu.

Rámce upravujúce subjektívnu zodpovednosť, v ktorých sú jasne stanovené povinnosti týkajúce sa kybernetickej bezpečnosti, umožňujú prevádzkovateľom určiť, čo musia urobiť, aby sa vyhli dôsledkom zodpovednosti.

⁵⁹ Správa o zodpovednosti za umelú inteligenciu a za iné nové technológie, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

V rámci smernice o zodpovednosti za výrobky by sa mohla dostať do popredia otázka, či výrobca mohol predpokladať určité zmeny vzhľadom na racionálne predpokladané použitie výrobku. Je možné, že budeme napríklad čoraz častejšie počuť obranný argument, že k chybe došlo neskôr, podľa ktorého výrobca nenesie zodpovednosť, ak chyba neexistovala v čase, keď bol výrobok uvedený do obehu, alebo obranný argument, že ide o riziko spojené s vývojom (a teda že pri stave poznatkov v oblasti vývoja v danom čase sa táto chyba nedala predvídať). Zodpovednosť by sa okrem toho mohla obmedziť, pokiaľ poškodená strana nevykonáva príslušné bezpečnostné aktualizácie. To by sa mohlo potenciálne považovať za spoluzavinenie poškodenej osoby z nedbanlivosti, čo by viedlo k obmedzeniu zodpovednosti výrobcu. Keby prevládla koncepcia racionálne predpokladaného použitia a otázka spoluzavinenia z nedbanlivosti, ako je napríklad nestiahnutie bezpečnostnej aktualizácie, pre poškodené osoby by to mohlo znamenať, že získať náhradu škody spôsobenej chybou vo výrobku bude zložitejšie.

Autonómnosť a nepriehľadnosť: Pokiaľ sú aplikácie umelej inteligencie schopné konať autonómne, plnia svoju úlohu bez toho, aby bol každý krok vopred definovaný, a fungujú viac menej bez bezprostredného ovládania človekom alebo ľudského dohľadu. Pochopiť algoritmy založené na strojovom učení môže byť ťažké, ak nie úplne nemožné (tzv. efekt čiernej skrinky).

Vzhľadom na efekt čiernej skrinky, ako aj vzhľadom na vyššie spomínanú zložitosť by získanie náhrady škody spôsobenej aplikáciami umelej inteligencie mohlo byť zložité. Potreba pochopiť algoritmus a údaje použité umelou inteligenciou si vyžaduje analytické kapacity a technické odborné znalosti, čo by mohli obete považovať za neúnosne nákladné. Prístup k algoritmu a údajom by navyše nemusel byť možný bez spolupráce potenciálne zodpovednej strany. V praxi by to pre obete znamenalo, že si nebudú schopné uplatniť nárok na náhradu škody. Okrem toho by nebolo jasné, ako preukázať zavinenie umelou inteligenciou, ktorá koná autonómne, alebo čo by sa malo považovať za zavinenie osobou, ktorá sa spolieha na používanie umelej inteligencie.

V rámci vnútroštátnych právnych predpisov sa už vypracovalo viacero riešení s cieľom znížiť dôkazné bremeno pre obete v podobných situáciách.

Pokiaľ ide o bezpečnosť výrobkov a zodpovednosť za výrobok, hlavnou zásadou zostáva, že je úlohou výrobcu zabezpečiť, aby boli všetky výrobky uvedené na trh bezpečné tak počas svojho životného cyklu, ako aj pri ich použitíach, ktoré možno racionálne očakávať. To znamená, že výrobca by musel zabezpečiť, aby výrobok používajúci umelú inteligenciu dodržiaval určité bezpečnostné parametre. Funkcie umelej inteligencie vo výrobkoch (bez ohľadu na to, či ide o automatické kosačky na trávnu alebo chirurgické roboty) sa nevylučujú s oprávnenými bezpečnostnými očakávaniami.

Autonómnosť môže ovplyvniť bezpečnosť výrobku, pretože môže podstatne zmeniť vlastnosti výrobku vrátane jeho bezpečnostných prvkov. Otázkou zostáva, za akých podmienok predlžujú zodpovednosť výrobcu prvky samoučenia a do akej miery by mal výrobca predvídať určité zmeny.

Pojem „uvedenie do obehu“, ktorý sa v súčasnosti používa v smernici o zodpovednosti za výrobky, by sa mohol prepracovať s cieľom zohľadniť skutočnosť, že vlastnosti výrobkov sa môžu zmeniť alebo zhoršiť, pričom toto prepracovanie by sa malo úzko koordinovať s príslušnými úpravami bezpečnostného rámca Únie. Mohlo by to navyše pomôcť objasniť, kto je zodpovedný za akékoľvek zmeny, ktoré sa na výrobku vykonajú.

Podľa správy⁶⁰ formácie pre nové technológie v rámci expertnej skupiny pre zodpovednosť a nové technológie by fungovanie niektorých autonómnych zariadení a služieb v oblasti umelej inteligencie mohlo z hľadiska zodpovednosti predstavovať osobitný rizikový profil, pretože môžu spôsobiť značné škody na dôležitých právnych záujmoch, ako je život, zdravie a majetok, a vystaviť verejnosť rizikám. Mohlo by sa to týkať najmä zariadení umelej inteligencie, ktoré sa pohybujú vo verejných priestoroch (napr. plne autonómne vozidlá, drony⁶¹ a roboty na doručovanie balíkov), alebo služieb založených na umelej inteligencii s podobnými rizikami (napr. služby riadenia dopravy, ktorými sa usmerňujú alebo kontrolujú vozidlá, alebo riadenie distribúcie energie). Výzvy spojené s autonómnosťou a nepriehľadnosťou vnútroštátnych právnych predpisov o občianskoprávnej zodpovednosti by sa mohli riešiť na základe prístupu založeného na posúdení rizika. Vďaka systémom objektívnej zodpovednosti by sa dalo zabezpečiť, aby bola obeť odškodnená zakaždým, keď sa riziko zhmotní, a to bez ohľadu na zavinenie. Bolo by potrebné starostlivo posúdiť, aký bude mať výber objektívne zodpovednej osoby za takéto operácie dosah na vývoj a využívanie umelej inteligencie, a zvážiť prístup založený na riziku.

Pokiaľ ide o prevádzkovanie aplikácií umelej inteligencie so špecifickým rizikovým profilom, Komisia skúma, či a v akom rozsahu je na dosiahnutie účinného odškodnenia možných obetí potrebná objektívna zodpovednosť tak, ako sa stanovuje vo vnútroštátnych právnych predpisoch pre podobné riziká, ktorým je vystavená verejnosť (napríklad v prípade prevádzkovaných motorových vozidiel, lietadiel alebo jadrových elektrární). Komisia sa tiež snaží zistiť názory na prepojenie objektívnej zodpovednosti s prípadnou povinnosťou uzavrieť dostupné poistenie podľa vzoru smernice o poistení motorových vozidiel, aby došlo k odškodneniu bez ohľadu na platobnú schopnosť zodpovednej osoby a aby sa mohli znížiť náklady na škodu.

V prípade prevádzky všetkých ostatných aplikácií umelej inteligencie, ktoré by predstavovali veľkú väčšinu aplikácií umelej inteligencie, Komisia uvažuje nad tým, či by sa nemalo upraviť dôkazné bremeno, pokiaľ ide o príčinnú súvislosť a zavinenie. V tejto súvislosti sa v správe⁶² vypracovanej formáciou pre nové technológie v rámci expertnej skupiny pre zodpovednosť a nové technológie poukázalo na problematickú situáciu, keď potenciálne zodpovedná strana nechová údaje relevantné pre posúdenie zodpovednosti alebo nie je ochotná poskytnúť ich obeť.

4. Záver

S novými digitálnymi technológiami, akými sú umelá inteligencia, internet vecí a robotika, vznikajú z hľadiska bezpečnosti výrobkov a zodpovednosti nové výzvy, ako je prepojitelnosť, autonómnosť, závislosť od údajov, nepriehľadnosť, zložitosť výrobkov a systémov, aktualizácie softvéru a zložitejšie riadenie bezpečnosti a hodnotové reťazce.

V platných právnych predpisoch v oblasti bezpečnosti výrobkov je potrebné riešiť viaceré nedostatky, a to najmä v smernici o všeobecnej bezpečnosti výrobkov, smernici o strojových

⁶⁰ Správa o zodpovednosti za umelú inteligenciu a za iné nové technológie, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

⁶¹ Porovnaj so systémami bezpilotných lietadiel, na ktoré sa odkazuje vo vykonávacom nariadení Komisie (EÚ) 2019/947 z 24. mája 2019 o pravidlách a postupoch prevádzky bezpilotných lietadiel.

⁶² Správa o zodpovednosti za umelú inteligenciu a za iné vznikajúce technológie, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

zariadeniach, smernici o rádiových zariadeniach a novom legislatívnom rámci. Jednotlivé právne predpisy v tomto rámci bude potrebné konzistentne a harmonizovane prispôbiť.

Nové výzvy z hľadiska bezpečnosti prinášajú aj nové výzvy z hľadiska zodpovednosti. Tieto výzvy súvisiace so zodpovednosťou je nutné riešiť, aby sa zabezpečila rovnaká úroveň ochrany ako v prípade obetí tradičných technológií, pričom sa musí zachovať rovnováha s potrebami technologickej inovácie. Vďaka tomu sa bude dať vybudovať dôvera v tieto nové digitálne technológie a zabezpečiť investičná stabilita.

Hoci sú existujúce právne predpisy Únie a vnútroštátne právne predpisy týkajúce sa zodpovednosti v zásade schopné poradiť si s novými technológiami, vzhľadom na rozmer a spojený účinok výziev vyplývajúcich z umelej inteligencie by sa mohlo sťažiť odškodňovanie obetí vo všetkých prípadoch, v ktorých by bolo odôvodnené⁶³. Rozdelenie nákladov v prípade vzniku škody môže byť preto podľa súčasných pravidiel nespravodlivé alebo neefektívne. S cieľom napraviť túto situáciu a vyriešiť potenciálne neistoty v súčasnom rámci by sa mohli zvažovať vhodné iniciatívy EÚ na určité úpravy smernice o zodpovednosti za výrobky a vnútroštátnych režimov, ku ktorým by sa cielene pristupovalo na základe posúdenia rizika, t. j. s prihliadnutím na to, že rôzne aplikácie umelej inteligencie predstavujú odlišné riziká.

⁶³ Pozri správu formácie pre nové technológie, s. 3, a politické odporúčanie 27.2 expertnej skupiny na vysokej úrovni pre umelú inteligenciu.