EVROPSKÁ
KOMISE

V Bruselu dne 19.2.2020
COM(2020) 64 final

ZPRÁVA KOMISE EVROPSKÉMU PARLAMENTU, RADĚ A EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU

Zpráva o dopadech umělé inteligence, internetu věcí a robotiky na bezpečnost a odpovědnost

ZPRÁVA O DOPADECH UMĚLÉ INTELIGENCE, INTERNETU VĚCÍ A ROBOTIKY NA BEZPEČNOST A ODPOVĚDNOST

1. Úvod

Umělá inteligence (AI)[1], internet věcí (IoT)[2] a robotika vytvoří v naší společnosti nové příležitosti a přinesou jí výhody. Komise uznává význam a potenciál těchto technologií a potřebu významných investic v těchto oblastech.[3] Je odhodlána učinit z Evropy v oblasti umělé inteligence, internetu věcí a robotiky světovou jedničku. K dosažení tohoto cíle je nutný jasný a předvídatelný právní rámec, který pokryje související technologické výzvy.

1.1 Stávající rámec pro bezpečnost a odpovědnost

Obecným účelem právních rámců pro bezpečnost a odpovědnost je zajistit, aby všechny výrobky a služby, včetně těch, které integrují vznikající digitální technologie, fungovaly bezpečně, spolehlivě a předvídatelně a aby byla účinně odstraňována vzniklá škoda. Vysoká úroveň bezpečnosti výrobků a systémů, které integrují nové digitální technologie, spolu s robustními mechanismy pro napravení vzniklé škody (tj. rámcem odpovědnosti) přispívají k lepší ochraně spotřebitelů. Rovněž vytvářejí důvěru v tyto technologie, což je předpokladem jejich přijetí ze strany průmyslu a uživatelů. To zase posílí konkurenceschopnost našeho průmyslu a přispěje k dosažení unijních cílů[4]. Jasný rámec pro bezpečnost a odpovědnost je obzvláště důležitý při nástupu nových technologií, jako jsou umělá inteligence, internet věcí a robotika, a to jak pro zajištění ochrany spotřebitelů, tak pro právní jistotu podniků.

Unie má spolehlivý regulační rámec pro bezpečnost a odpovědnost za výrobky a spolehlivý soubor bezpečnostních norem doplněný vnitrostátní, neharmonizovanou legislativou pro odpovědnost. Společně na jednotném trhu zajišťují dobré životní podmínky občanů a podporují inovace a technologické využití. Umělá inteligence, internet věcí a robotika však mění vlastnosti mnoha výrobků a služeb.

Ve sdělení o umělé inteligenci pro Evropu[5], které bylo přijato dne 25. dubna 2018, bylo uvedeno, že Komise předloží zprávu posuzující dopady vznikajících digitálních technologií na stávající rámce v oblasti bezpečnosti a odpovědnosti. Tato zpráva si klade za cíl určit a posoudit širší dopady na rámce pro odpovědnost a bezpečnost pro umělou inteligenci, internet věcí a robotiku a jejich potenciální nedostatky. Směry obsažené v této zprávě připojené k bílé knize o umělé inteligenci jsou uvedeny k diskusi a jsou součástí širších konzultací se zúčastněnými stranami. Oddíl týkající se bezpečnosti vychází z posouzení[6]

---

1 Definice odborné skupiny na vysoké úrovni pro umělou inteligenci (AI HLEG) je k dispozici na adrese https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

2 Definice internetu věcí uvedená v doporučení ITU-T Y.2060 je k dispozici 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 https://ec.europa.eu/growth/industry/policy_cs

5 https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018DC0237&from=EN. Pracovní dokument útvarů Komise (2018) 137 (https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137) prvně zmapoval výzvy v oblasti odpovědnosti v oblasti vznikajících digitálních technologií.

6 Pracovní dokument útvarů Komise SWD(2018) 161 final.

směrnice o strojních zařízeních[7] a z práce příslušných skupin odborníků[8]. Oddíl týkající se odpovědnosti vychází z posouzení[9] směrnice o odpovědnosti za výrobky[10], příspěvků od skupin odborníků[11] a kontaktu se zúčastněnými stranami. Cílem této zprávy není poskytnout vyčerpávající přehled o stávajících předpisech pro bezpečnost a odpovědnost, ale zaměřuje se na klíčové otázky, které byly dosud identifikovány.

1.2 Charakteristika technologií využívajících umělou inteligenci, internet věcí a robotiku

Umělá inteligence, internet věcí a robotika mají mnoho společného. Díky spojení **konektivity**, **autonomie** a **závislosti na datech** mohou plnit úkoly s malým zapojením lidské kontroly a dohledu nebo i bez nich. Systémy využívající umělou inteligenci též mohou zlepšovat svou výkonnost učením se ze svých zkušeností. Jejich **složitost** se odráží jak v množství hospodářských subjektů zapojených do **dodavatelského řetězce**, tak v celé řadě součástí, dílů, softwaru, systémů nebo služeb, které společně tvoří nové technologické ekosystémy. Je též třeba vzít v potaz jejich **otevřenost** k aktualizacím a modernizaci po jejich uvedení na trh. Velké množství údajů, spoléhání se na algoritmy a **neprůhlednost** rozhodování umělé inteligence snižují předvídatelnost chování produktů, které ji využívají, a ztěžují porozumění při hledání možných příčin škody. Konektivita a otevřenost též mohou vystavit produkty umělé inteligence a internetu věcí **kybernetickým hrozbám**.

1.3 Příležitosti vytvořené umělou inteligencí, internetem věcí a robotikou

Zvýšení důvěry uživatelů ve vznikající technologie a jejich společenské akceptace, zlepšování produktů, postupů a obchodních modelů a přispění k vyšší efektivitě evropských výrobců – to jsou pouze některé z příležitostí, které umělá inteligence, internet věcí a robotika nabízejí.

Kromě zvýšení produktivity a efektivity si od umělé inteligence rovněž slibujeme, že člověku umožní dosáhnout vyšší inteligence, než jaké byl dosud schopen, že otevře dveře novým objevům a pomůže vyřešit některé z největších světových výzev: od léčby chronických onemocnění, předcházení epidemiím či snižování míry úmrtnosti při dopravních nehodách po boj proti klimatickým změnám či předvídání bezpečnostních hrozeb v kyberprostoru.

Tyto technologie mohou přinést mnoho výhod zlepšením bezpečnosti výrobků, čímž sníží jejich náchylnost k určitým rizikům. Například propojená a automatizovaná vozidla by mohla

---

[7] Směrnice 2006/42/ES.

[8] Síť pro bezpečnost spotřebitelů, jak je stanovena ve směrnici 2001/95/ES o obecné bezpečnosti výrobků, směrnici 2006/42/EC o strojních zařízeních a směrnici 2014/53/EU o rádiových zařízeních, skupiny odborníků složených z členských států, průmyslu a dalších zúčastněných stran, jako jsou sdružení spotřebitelů.

[9] COM(2018) 246 final.

[10] Směrnice 85/374/EHS.

[11] Skupina odborníků pro odpovědnost a nové technologie byla vytvořena proto, aby Komisi poskytla odborné znalosti o použitelnosti směrnice o odpovědnosti za výrobky a vnitrostátních a o použitelnosti vnitrostátních pravidel týkajících se občanskoprávní odpovědnosti, a aby přispěla při tvorbě hlavních zásad pro možné úpravy platných právních předpisů týkajících se nových technologií. Skládá se ze dvou útvarů, „útvaru pro odpovědnost za výrobky“ a „útvaru pro nové technologie“, viz http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1.
Zpráva „Sestava pro nové technologie“ o odpovědnosti za umělou inteligenci a další vznikající technologie, viz https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

zvýšit bezpečnost silničního provozu, neboť většina dopravních nehod je v současnosti způsobena lidskými chybami[12]. Systémy internetu věcí jsou navíc koncipovány tak, aby získávaly a zpracovávaly obrovské množství dat z různých zdrojů. Tato zvýšená úroveň informací může být využita tak, aby se výrobky mohly samy přizpůsobit, a staly se tak bezpečnějšími. Nové technologie mohou přispět k efektivnějšímu stahování výrobků z oběhu, neboť by výrobky mohly uživatele samy upozornit na to, jak se vyhnout bezpečnostnímu problému[13]. Pokud se při používání propojeného výrobku vyskytne bezpečnostní riziko, mohou výrobci komunikovat přímo s uživateli, jednak aby je varovali před riziky, jednak aby případně problém přímo vyřešili, například bezpečnostní aktualizací. Například během stažení jednoho ze svých zařízení v roce 2017 provedl výrobce chytrého telefonu aktualizaci softwaru, která snížila kapacitu baterie těchto stažených telefonů na nulu[14], aby uživatelé tato nebezpečná zařízení přestali používat.

Nové technologie mohou dále přispět ke zlepšení sledovatelnosti výrobků. Například díky propojenosti internetu věcí mohou podniky a orgány pro dozor nad trhem sledovat nebezpečné výrobky a identifikovat rizika napříč dodavatelskými řetězci[15].

Společně s příležitostmi mohou umělá inteligence, internet věcí a robotika přinést ekonomice a společnosti rovněž riziko poškození právně chráněných zájmů jak hmotných, tak nehmotných. Toto riziko se zvýší spolu s rozšířením jejich využití. V této souvislosti je nezbytné analyzovat, zda a do jaké míry je stávající právní rámec pro bezpečnost a odpovědnost nadále vhodný k ochraně uživatelů.

2. Bezpečnost

Sdělení Komise o „Budování důvěry v umělou inteligenci zaměřenou na člověka“ uvádí, že by ***nedílnou součástí systémů umělé inteligence měly již od návrhu být mechanismy bezpečnosti a zabezpečení, které zaručí, aby byly tyto systémy v každé fázi prokazatelně bezpečné,*** *a aby chránily* ***fyzické i psychické zdraví*** *všech zúčastněných*[16].

Posouzení právních předpisů Unie pro bezpečnost výrobků v tomto oddíle analyzuje, zda stávající právní rámec Unie obsahuje příslušné prvky pro zajištění, aby nově vznikající technologie a zejména systémy umělé inteligence zahrnovaly bezpečnost a zabezpečení již od návrhu.

Tato zpráva se zabývá především směrnicí o obecné bezpečnosti výrobků[17] a harmonizovanými právními předpisy v oblasti výrobků, které se řídí horizontálními pravidly

---

[12] Podle odhadů je asi 90 % dopravních nehod na silnicích způsobeno lidskou chybou. Viz zpráva Komise nazvaná „Záchrana životů: Zvyšování bezpečnosti vozidel v EU“ (COM(2016) 787 final).

[13] Řidič vozidla může být například upozorněn, aby zpomalil před místem nehody.

[14] OECD (2018), „Měření a maximalizace dopadu stažení výrobků na celosvětové úrovni: zpráva z pracovního semináře OECD“, *OECD Science, Technology and Industry Policy Papers* , č. 56, OECD Publishing, Paříž, https://doi.org/10.1787/ab757416-en.

[15] OECD (2018), „Zlepšení účinnosti stahování výrobků z oběhu v celosvětovém měřítku: podkladová zpráva OECD“, *OECD Science, Technology and Industry Policy Papers*, č. 58, OECD Publishing, Paříž, https://doi.org/10.1787/ab757416-en.

[16] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Budování důvěry v umělou inteligenci zaměřenou na člověka, Brusel, 8. 4. 2019 COM (2019) 168 final.

[17] Směrnice Evropského parlamentu a Rady 2001/95/ES ze dne 3. prosince 2001 o obecné bezpečnosti výrobků (Úř. věst. L 11, 15.1.2002, s. 4).

„nového přístupu“[18], případně „nového právního rámce“ (dále jen „právní předpisy nebo rámec Unie v oblasti bezpečnosti výrobků“)[19]. Horizontální pravidla zajišťují soudržnost mezi odvětvovými pravidly pro bezpečnost výrobků.

Cílem právních předpisů Unie o bezpečnosti výrobků je zajistit, aby výrobky uváděné na trh Unie splňovaly vysoké požadavky na zdraví, bezpečnost a ochranu životního prostředí a aby se tyto výrobky mohly volně pohybovat v celé Unii. Odvětvové právní předpisy[20] jsou doplněny směrnicí o obecné bezpečnosti výrobků[21], která vyžaduje, aby všechny spotřební výrobky byly bezpečné, i když nejsou regulovány odvětvovými právními předpisy Unie. Pravidla bezpečnosti doplňují dozor nad trhem a pravomoci svěřené vnitrostátním orgánům podle nařízení o dozoru nad trhem[22] a směrnice o obecné bezpečnosti výrobků[23]. V dopravě existují další pravidla Unie a členských států pro uvedení motorového vozidla[24], letadla či plavidla do provozu, jakož i jasná pravidla, která upravují bezpečnost během provozu, včetně úkolů pro provozovatele a pro orgány týkající se dozoru.

Evropská normalizace je rovněž zásadním prvkem právních předpisů Unie v oblasti bezpečnosti výrobků. Vzhledem ke globální povaze digitalizace a vznikajících digitálních technologií je mezinárodní spolupráce v oblasti normalizace pro konkurenceschopnost evropského průmyslu otázkou zvláštního významu.

Velká část rámce Unie pro bezpečnost výrobků byla vypracována před vznikem digitálních technologií, jako jsou umělá inteligence, internet věcí nebo robotika. Neobsahuje proto vždy ustanovení, která by nové výzvy a rizika těchto vznikajících technologií výslovně řešila. Avšak i když je stávající rámec pro bezpečnost výrobků technologicky neutrální, neznamená to, že by se na výrobky obsahující tyto technologie nevztahoval. Navíc následné legislativní akty, které jsou součástí tohoto rámce, například v oblasti zdravotnických prostředků nebo automobilů, se již výslovně zabývají některými aspekty vznikajících digitálních technologií, jako jsou např. automatizovaná rozhodnutí, software jako samostatný výrobek a konektivita.

[18] Úř. věst. C 136, 4.6.1985, s. 1.

[19] Nařízení (ES) č. 2008/765 a rozhodnutí (ES) č. 2008/768

[20] Toto schéma nezahrnuje právní předpisy Unie v oblasti dopravy a automobilů.

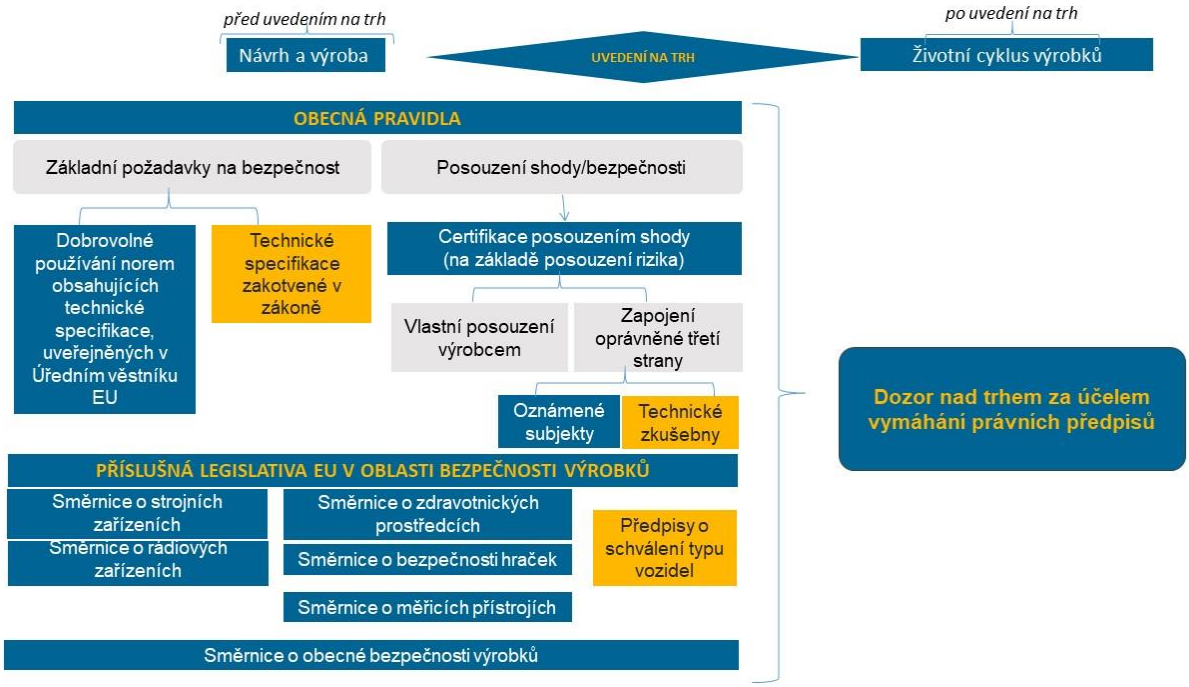
[21] Směrnice Evropského parlamentu a Rady 2001/95/ES ze dne 3. prosince 2001 o obecné bezpečnosti výrobků (Úř. věst. L 11, 15.1.2002, s. 4).

[22] Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93, Úř. věst. L 218, 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj a od roku 2021 dále nařízení Evropského parlamentu a Rady (EU) 2019/1020 ze dne 20. června 2019 o dozoru nad trhem a souladu výrobků s předpisy a o změně směrnice 2004/42/ES a nařízení (ES) č. 765/2008 a (EU) č. 305/201,1 Úř. věst. L 169, 25.6.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/1020/oj

[23] Čl. 8 odst. 1 písm. b) bod 3 směrnice o obecné bezpečnosti výrobků

[24] Například směrnice 2007/46/ES – schvalování motorových vozidel a jejich přípojných vozidel, jakož i systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla a nařízení Evropského parlamentu a Rady (EU) 2018/858 ze dne 30. května 2018 o schvalování motorových vozidel a jejich přípojných vozidel, jakož i systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla a o dozoru nad trhem s nimi, kterým se mění nařízení (ES) č. 715/2007 a (ES) č. 595/2009 a zrušuje směrnice 2007/46/ES

Logika stávajících právních předpisů Unie v oblasti bezpečnosti výrobků[25]



Výzvy, které vznikající digitální technologie přináší do rámce pro bezpečnost výrobků v Unii, jsou uvedeny níže.

Konektivita je klíčovým prvkem stále rostoucího počtu výrobků a služeb. Tento prvek je z hlediska tradičního pojetí bezpečnosti problematický, neboť konektivita může ohrozit bezpečnost výrobku přímo, nebo nepřímo tím, že díky ní lze produkt napadnout, což může vést k bezpečnostním hrozbám a ovlivnit bezpečnost uživatelů.

Příkladem je oznámení systému rychlého varování EU ze strany Islandu týkající se chytrých hodinek pro děti[26]. Tento výrobek by dítěti, které ho nosí, nezpůsobil přímou škodu, ale v důsledku absence minimální úrovně zabezpečení může být snadno použit jako nástroj pro získání přístupu k dítěti. Vzhledem k tomu, že jedním z cílů výrobku je chránit bezpečnost dětí tím, že umožňuje sledovat jejich lokaci, spotřebitel by očekával, že nebude obsahovat bezpečností rizika, která by mohla ohrozit bezpečnost dítěte tím, že umožní dítě sledovat nebo kontaktovat komukoli.

Další příklad uvádí oznámení předložené Německem ohledně osobního automobilu[27]. Rádio v tomto vozidle může obsahovat určité bezpečnostní nedostatky v bezpečnosti softwaru, které umožňují neoprávněným třetím stranám přístup do propojených řídicích systémů vozidla. Pokud by tyto nedostatky v zabezpečení softwaru byly zneužity třetí stranou k nekalým účelům, mohlo by dojít k dopravní nehodě.

Také průmyslové aplikace mohou být vystaveny kybernetickým hrozbám s potenciálně výrazným dopadem na bezpečnost osob, postrádají-li nezbytnou míru zabezpečení. Tak tomu

[25] Toto schéma nezahrnuje požadavky na právní předpisy týkající se životního cyklu výrobku, tj. používání a údržby, je přiloženo pouze pro ilustraci.

[26] Oznámení v systému RAPEX z Islandu zveřejněné na internetových stránkách EU Safety Gate (A12/0157/19)

[27] Oznámení v systému RAPEX z Německa zveřejněné na internetových stránkách EU Safety Gate (A12/1671/15)

může být například v případě kybernetických útoků na kritický kontrolní systém průmyslového závodu s cílem vyvolat explozi, která by mohla vést ke ztrátám na životech.

Právní předpisy Unie v oblasti bezpečnosti výrobků obecně nestanoví konkrétní povinné základní požadavky na zabezpečení vůči kybernetickým hrozbám s dopadem na bezpečnost uživatelů. Ustanovení týkající se bezpečnostních aspektů však existují v nařízení o zdravotnických prostředcích[28], směrnici o měřicích přístrojích[29], směrnici o rádiových zařízeních[30] nebo v právních předpisech týkajících se schvalování typu vozidel[31]. Akt o kybernetické bezpečnosti[32] zavádí dobrovolný rámec pro certifikaci produktů, služeb a procesů v oblasti informačních a komunikačních technologií (IKT) z hlediska kybernetické bezpečnosti, přičemž příslušné právní předpisy Unie v oblasti bezpečnosti výrobků stanoví povinné požadavky.

Riziko ztráty konektivity u vznikajících digitálních technologií může navíc obnášet i rizika spojená s bezpečností. Pokud například propojený požární poplašné zařízení ztratí připojení, hrozí, že uživatele v případě požáru neupozorní.

Bezpečnost je ve stávajících právních předpisech Unie v oblasti bezpečnosti výrobků cílem veřejné politiky. Koncepce bezpečnosti je spojena s používáním výrobku a riziky, např. mechanickým ohrožením, nebezpečím úrazu elektrickým proudem atd., která je třeba řešit, aby byl výrobek bezpečný. Je třeba poznamenat, že v závislosti na právním předpisu Unie o bezpečnosti výrobků se použití výrobku vztahuje nejen na zamýšlené použití, ale také na předvídatelné použití a v některých případech, například ve směrnici o strojních zařízeních[33], i na důvodně předvídatelné nesprávné použití.

Koncepce bezpečnosti ve stávajících právních předpisech Unie v oblasti bezpečnosti výrobků je v souladu s rozšířenou koncepcí bezpečnosti s cílem chránit spotřebitele a uživatele. Pojem bezpečnost výrobků tak zahrnuje ochranu před všemi druhy rizik vyplývajících z výrobku, včetně nejen mechanických, chemických a elektrických rizik, ale i kybernetických rizik a rizik souvisejících se ztrátou konektivity zařízení.

Za účelem zajištění lepší ochrany uživatelů a větší právní jistoty je možné zvážit zahrnutí výslovných ustanovení do příslušných právních předpisů Unie.

Jedním z hlavních rysů umělé inteligence je **autonomie**[34]. Důsledky nezamýšlených výstupů umělé inteligence by mohly poškodit uživatele a dotčené osoby.

V míře, ve které lze předvídat budoucí „chování“ výrobků umělé inteligence prostřednictvím posouzení rizik provedeného výrobcem před jejich uvedením na trh, stanoví rámec Unie pro

[28] Nařízení (EU) 2017/745 o zdravotnických prostředcích.
[29] Směrnice 2014/32/EU, která se zabývá dodáváním měřidel na trh.
[30] Směrnice o rádiových zařízeních 2014/53/EU.
[31] Směrnice 2007/46/ES – schvalování motorových vozidel a jejich přípojných vozidel, jakož i systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla. Tato směrnice bude zrušena a nahrazena nařízením (EU) 2018/858 o schvalování motorových vozidel a jejich přípojných vozidel, jakož i systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla a o dozoru nad trhem s nimi, o změně nařízení (ES) č. 715/2007 a č. 595/2009 a o zrušení směrnice 2007/46/ES s účinkem ode dne 1. září 2020.
[32] Nařízení (EU) 2019/881.
[33] Směrnice 2006/42/ES – o strojních zařízeních.
[34] Ačkoli výrobky založené na umělé inteligenci mohou jednat autonomně vnímáním svého okolí a aniž by se řídily souborem předem stanovených pokynů, jejich chování je vymezeno přednastaveným cílem a dalšími relevantními volbami stanovenými vývojáři při návrhu systému. „

bezpečnost výrobků již teď povinnost výrobců zohlednit při posuzování rizik to, jak budou výrobky „používány“[35] po celou dobu jejich životnosti. Rovněž předpokládá, že výrobci musí uživatelům poskytnout pokyny a bezpečnostní informace nebo varování[36]. V této souvislosti například směrnice o rádiových zařízeních[37] požaduje, aby výrobce přiložil návod s informacemi o tom, jak používat rádiové zařízení v souladu s jeho zamýšleným použitím.

V budoucnu se mohou vyskytnout i situace, kdy výstupy systémů umělé inteligence nebude možné předem plně určit. V takové situaci již posouzení rizik provedené před uvedením výrobku na trh nemusí odrážet použití, fungování nebo chování výrobku. V těchto případech, pokud se zamýšlené použití původně předpokládané výrobcem změní[38] v důsledku autonomního chování a soulad s bezpečnostními požadavky je narušen, lze u takového samoučícího výrobku uvažovat o novém posouzení rizik[39].

Pokud se výrobce dozví, že výrobek kdykoliv během svého životního cyklu představuje riziko, které má dopad na bezpečnost, musí podle stávajícího rámce okamžitě informovat příslušné orgány a přijmout opatření, aby se rizikům pro uživatele předešlo[40].

Kromě posouzení rizik provedeného před uvedením výrobku na trh by mohl být zaveden nový postup posuzování rizik pro výrobky, u kterých během jejich životnosti dochází k významným změnám, např. ke změně funkce výrobku, kterou výrobce v původním posouzení rizik nepředpokládal. Toto posouzení by mělo být zaměřeno na dopady na bezpečnost způsobené autonomním chováním výrobku po celou dobu jeho životnosti. Posouzení rizik by měl provádět příslušný hospodářský subjekt. Kromě toho by příslušné právní předpisy Unie mohly zahrnovat posílené požadavky na výrobce týkající se pokynů a varování pro uživatele.

Podobná posouzení rizik jsou již vyžadována v právních předpisech v oblasti dopravy[41]; například v právních předpisech v oblasti železniční dopravy, je-li železniční vozidlo po

---

[35] Podle právních předpisů Unie o bezpečnosti výrobků provádějí výrobci posouzení rizik na základě zamýšleného použití výrobku, jeho předvídatelného použití anebo jeho důvodně předvídatelného nesprávného použití.

[36] Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES ze dne 9. července 2008 o společném rámci pro uvádění výrobků na trh a o zrušení rozhodnutí Rady 93/465/EHS, Úř. věst. L 218, 13.8.2008, s. 82. Článek R2.7 přílohy I zní: „*Výrobci zajistí, aby byl k výrobku přiložen návod a bezpečnostní informace v jazyce snadno srozumitelném spotřebitelům a ostatním konečným uživatelům, který stanoví dotčený členský stát.*“

[37] Čl. 10 odst. 8 odkazující na pokyny pro koncového uživatele a přílohu VI, která odkazuje na EU prohlášení o shodě

[38] „Samoučící“ se dosud v souvislosti s umělou inteligencí používá především k označení toho, že je stroj schopen učit se během svého tréninku; není dosud požadováno, aby se stroje využívající umělou inteligenci dále učily i po svém nasazení do provozu; naopak, zejména v oblasti zdravotní péče se obvykle stroje využívající umělou inteligenci po úspěšném ukončení tréninku učit přestávají. V této fázi tedy autonomní chování vycházející z umělé inteligence neznamená, že výrobek plní úkoly, které tvůrci nezamýšleli.

[39] Toto je v souladu s oddílem 2.1 „Modré příručky“ k provádění pravidel EU pro výrobky 2016.

[40] Článek 5 směrnice Evropského parlamentu a Rady 2001/95/ES ze dne 3. prosince 2001 o obecné bezpečnosti výrobků.

[41] V případě jakékoli změny železničního systému, která by mohla mít dopad na bezpečnost (např. technická, provozní změna nebo také organizační změna, která by mohla mít dopad na provoz nebo údržbu), je postup, který je třeba dodržet, popsán v příloze I prováděcího nařízení (EU) 2015/1136 (Úř. věst. L 185, 14.7.2015, s. 6).
V případě „významné změny“ by měla být předkladateli předložena zpráva o posouzení bezpečnosti, kterou provede nezávislý „hodnotící orgán“ (tím může být vnitrostátní bezpečnostní orgán nebo jiný technicky způsobilý orgán).
Po provedení analýzy rizik navrhovatel změny uplatní vhodná opatření ke zmírnění rizik (pokud je navrhovatelem železniční podnik nebo správce infrastruktury, uplatňování nařízení je součástí jeho systému zajišťování bezpečnosti, na který dohlíží vnitrostátní bezpečnostní orgán).

vydání osvědčení změněno, je původci změny uložen zvláštní postup s jasně definovanými pravidly ke stanovení, zda je nutné se obrátit na příslušný orgán, či nikoli.

Schopnost samostatného učení u výrobků a systémů umělé inteligence může stroji umožnit přijímání rozhodnutí, která se odchylují od toho, co výrobci původně zamýšleli, a v důsledku toho též od očekávání jejich uživatelů. To vyvolává otázky o lidské kontrole, která by měla umožnit volbu, zda a jak za účelem plnění cílů stanovených člověkem přenechat rozhodnutí produktům a systémům umělé inteligence[42]. Stávající právní předpisy Unie v oblasti bezpečnosti výrobků výslovně neřeší lidský dohled v souvislosti s produkty a systémy umělé inteligence založenými na samostatném učení[43].

Příslušné právní předpisy Unie mohou předvídat zvláštní požadavky na lidský dohled jakožto bezpečnostní záruku, od návrhu výrobku a po celou dobu životnosti výrobků a systémů umělé inteligence.

Budoucí „chování“ aplikací umělé inteligence by mohlo pro uživatele představovat **riziko pro duševní zdraví**[44] vyplývající například z jejich spolupráce s humanoidními roboty a systémy umělé inteligence ať už doma, nebo v pracovním prostředí. V tomto ohledu je dnes bezpečnost obecně chápána ve smyslu vnímané hrozby tělesné újmy pro uživatele, kterou by mohla vznikající digitální technologie způsobit. Zároveň jsou v právním rámci Unie bezpečné výrobky definovány jako výrobky, které nepředstavují žádné riziko, nebo jen minimální riziko pro bezpečnost a zdraví osob. Obecně se má za to, že definice zdraví zahrnuje jak tělesnou, tak duševní pohodu. Rizika spojená s duševním zdravím by však měla být v legislativním rámci výslovně zahrnuta do pojmu „bezpečnost výrobků“.

Například autonomie by neměla způsobovat nadměrný stres a nepohodlí po delší dobu a neměla by vést k poškození duševního zdraví. V tomto ohledu se má za to, že faktory, které pozitivně ovlivňují pocit bezpečí u starších osob[45], jsou: pocit bezpečného vztahu se zdravotnickým personálem poskytujícím péči, kontrola nad každodenní rutinou a informovanost ohledně každodenní rutiny. Aby se předešlo rizikům pro duševní zdraví, měli by výrobci robotů pracujících se staršími lidmi tyto faktory vzít v úvahu.

Z hlediska působnosti příslušných právních předpisů EU by mohla být zvážena výslovná povinnost výrobců humanoidních robotů s umělou inteligencí a některých dalších výrobků explicitně zohlednit nehmotnou újmu, kterou by jejich výrobky mohly způsobit uživatelům, obzvláště pak zranitelným uživatelům, jako jsou například starší osoby v pečovatelském prostředí.

Další základní vlastností výrobků a systémů založených na umělé inteligenci je **závislost na datech**. Přesnost a relevantnost údajů jsou zásadní pro zajištění toho, aby systémy a produkty založené na umělé inteligenci přijímaly rozhodnutí podle záměrů výrobce.

---

[42] Politická a investiční doporučení pro zajištění důvěryhodnosti umělé inteligence, odborná skupina na vysoké úrovni pro umělou inteligenci, červen 2019.

[43] To však nevylučuje, že v důsledku některých stávajících obecnějších povinností týkajících se uvádění výrobku na trh může být v určité situaci dohled nutný.

[44] Stanovy Světové zdravotnické organizace, první odrážka: „Zdraví je stavem úplné tělesné, duševní a sociální pohody, ne pouhou nepřítomností nemoci či vady.“ (https://www.who.int/about/who-we-are/constitution)

[45] Sociální roboti: Technologická, společenská a etická hlediska interakce mezi lidmi a roboty, s. 237–264, Research, Neziha Akalin, Annica Kritoffersson a Amy Loutfi, červenec 2019.

Právní předpisy Unie v oblasti bezpečnosti výrobků neřeší výslovně bezpečnostní rizika vyplývající z chybných údajů. Podle „použití“ výrobku by však výrobci měli během fáze návrhu a testování zvážit přesnost údajů a její význam pro bezpečnostní funkce.

Například systém založený na umělé inteligenci, který má odhalovat konkrétní objekty, může mít potíže s jejich rozpoznáváním za špatných světelných podmínek, a proto by při jejich návrhu měly být zahrnuty údaje pocházející ze zkoušek výrobků v typickém osvětlení i za špatných světelných podmínek.

Další příklad se týká zemědělských robotů, jako jsou roboti používaní na sklizeň ovoce, jejichž cílem je najít na stromech nebo na zemi zralé plody. Přestože související algoritmy již vykazují úspěšnost při rozpoznávání více než 90 %, mohla by chyba v souboru údajů, které tyto algoritmy používají, vést u těchto robotů ke špatnému rozhodnutí, v důsledku kterého může dojít ke zranění zvířete nebo osoby.

Vyvstává otázka, zda by právní předpisy Unie v oblasti bezpečnosti výrobků měly obsahovat konkrétní požadavky týkající se ohrožení bezpečnosti způsobené použitím chybných údajů ve fázi návrhu, jakož i mechanismy pro zajištění toho, aby byla po celou dobu používání produktů a systémů umělé inteligence kvalita údajů zachována.

Další zásadní vlastností některých výrobků a systémů založených na umělé inteligenci, která může vyplývat z jejich schopnosti zlepšovat svou výkonnost získáváním zkušeností, je **neprůhlednost**. U výrobků a systémů založených na umělé inteligenci lze v závislosti na metodickém přístupu charakterizovat různé stupně neprůhlednosti. To může vést k tomu, že proces rozhodování bude obtížné sledovat („efekt černé skříňky“). Člověk nemusí nutně chápat každý jednotlivý krok rozhodovacího procesu, avšak s rostoucí složitostí algoritmů umělé inteligence a jejich nasazením v kritických oblastech, je zásadně důležité, aby lidé měli možnost chápat, jakým způsobem systém dospěl ke svým algoritmickým rozhodnutím. Toto by bylo obzvláště důležité pro mechanismus následného vymáhání, neboť umožní donucovacím orgánům vysledovat odpovědnost za chování a volby systémů umělé inteligence. To uznává i sdělení Komise o budování důvěry v umělou inteligenci zaměřenou na člověka[46].

Právní předpisy Unie v oblasti bezpečnosti výrobků neřeší výslovně zvyšující se rizika vyplývající z neprůhlednosti systémů založených na algoritmech. Je proto nezbytné zvážit požadavky na transparentnost algoritmů, jakož i na spolehlivost, odpovědnost a případně lidský dohled a nezaujatost výsledků[47], zejména s ohledem na mechanismus následného vymáhání a pro vytvoření důvěry při používání těchto technologií. Jedním ze způsobů, jak tuto výzvu řešit, by bylo uložení povinnosti vývojářům algoritmů v případě nehody zveřejnit vývojové parametry a metadata souborů dat.

Další rizika, která mohou mít dopad na bezpečnost, jsou rizika, která vyplývají ze **složitosti výrobků a systémů**, neboť různé integrované součásti, zařízení a výrobky mohou mít navzájem vliv na své fungování (např. výrobky, které jsou součástí ekosystému chytré domácnosti).

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

[47] Na základě klíčových požadavků navržených expertní skupinou na vysoké úrovni pro etické pokyny pro důvěryhodnou umělou inteligenci: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

Tuto složitost již řeší bezpečnostní právní rámec Unie uvedený na začátku tohoto oddílu[48]. Zejména při posuzování rizik výrobku musí výrobce zvážit zamýšlené použití, předvídatelné použití a případně důvodně předvídatelné nesprávné použití.

Pokud v souvislosti s tímto **výrobce předpokládá, že jeho zařízení bude propojeno s jinými prostředky, se kterými bude interagovat, mělo by to být zohledněno při posuzování rizik**. Použití nebo nesprávné použití se určuje například na základě zkušeností s dřívějším použitím téhož druhu výrobku, z vyšetřování nehod nebo lidského chování.

Složitost systémů se rovněž konkrétněji řeší odvětvovými právními předpisy v oblasti bezpečnosti, jako je nařízení o zdravotnických prostředcích a do určité míry v právních předpisech o obecné bezpečnosti výrobků[49]. Například výrobce propojeného zařízení, které má být součástí ekosystému chytré domácnosti, by měl mít například rozumně předpokládat, že jeho výrobky budou mít dopad na bezpečnost jiných výrobků.

Kromě toho právní předpisy v oblasti dopravy řeší tuto složitost na systémové úrovni. U automobilů, vlaků a letadel se pro každou konstrukční část provádí schválení typu a certifikace stejně tak, jak je tomu v případě celého vozidla nebo letadla. Technická způsobilost vozidel, letová způsobilost letadel a interoperabilita železničního systému jsou součástí hodnocení jejich bezpečnosti. V dopravě musí být „systémy“ „povoleny“ orgánem, a to buď na základě posouzení shody s jasnými technickými požadavky třetí stranou, nebo po prokázání toho, jak jsou řešena rizika. Řešení jsou obecně kombinací úrovní „výrobku“ a „systému“.

Právní předpisy Unie v oblasti bezpečnosti výrobků, včetně právních předpisů v oblasti dopravy, již při řešení rizik, která mohou mít dopad na bezpečnost uživatelů, do určité míry složitost výrobků nebo systémů zohledňují.

Složité systémy často zahrnují **software**, který je základní součástí systému založeného na umělé inteligenci. V rámci počátečního posouzení rizik má obecně výrobce konečného výrobku povinnost předvídat rizika softwaru zabudovaného v tomto výrobku v době jeho uvedení na trh.

Některé právní předpisy Unie v oblasti bezpečnosti výrobků výslovně odkazují na software začleněný do výrobku. Například směrnice o strojních zařízeních[50] vyžaduje, aby závada v programovém vybavení ovládacího systému nevedla k nebezpečným situacím.

V právních předpisech Unie týkajících se bezpečnosti výrobků by aktualizace softwaru mohly být srovnatelné s údržbou z bezpečnostních důvodů za předpokladu, že podstatně nezmění výrobek, který je již uveden na trh, a nezavedou nová rizika, která nebyla uvedena v počátečním posouzení rizik. Pokud však aktualizace softwaru podstatně mění výrobek, do kterého byla stažena, celý výrobek by mohl být považován za nový výrobek a musel by být znovu posouzen soulad s příslušnými právními předpisy týkajícími se bezpečnosti výrobku v době provedení změny[51].

Pro samostatný software, který je uváděn na trh nebo nahrán po uvedení výrobku na trh, nemají obecně harmonizované právní předpisy Unie v oblasti bezpečnosti výrobků specifická

[48] Nařízení (ES) č. 2008/765 a rozhodnutí (ES) č. 2008/768 a harmonizované právní předpisy pro bezpečnost výrobků v jednotlivých odvětvích, např. směrnice 2006/42/ES o strojních zařízeních.

[49] Článek 2 směrnice o obecné bezpečnosti výrobků stanoví, že bezpečný výrobek musí brát v úvahu „vliv na jiné výrobky, jestliže lze rozumně předpokládat, že výrobek bude používán s jinými výrobky“.

[50] Oddíl 1.2.1 přílohy I směrnice o strojních zařízeních.

[51] „Modrá příručka“ k provádění pravidel EU pro výrobky, 2016;

ustanovení. Některé právní předpisy Unie však samostatný software řeší, jako například nařízení o zdravotnických prostředcích. Samostatný software nahraný do propojených výrobků, které komunikují prostřednictvím určitých rádiových modulů[52], může být rovněž upraven směrnicí o rádiových zařízeních prostřednictvím aktů v přenesené pravomoci. Tato směrnice vyžaduje, aby konkrétní kategorie nebo třídy rádiových zařízení podporovaly určité funkční charakteristiky, které zajišťují, že nahrání softwaru neohrozí jejich soulad s právními předpisy[53].

Ačkoli právní předpisy Unie týkající se bezpečnosti výrobků zohledňují bezpečnostní rizika vyplývající ze softwaru integrovaného ve výrobku v době jeho uvedení na trh a potenciálně následné aktualizace předvídané výrobcem, pro samostatný software (např. pro stahovatelné aplikace) mohou být zapotřebí zvláštní a případně výslovné požadavky. Zvláštní pozornost by měla být věnována samostatnému softwaru, který zajišťuje bezpečnostní funkce ve výrobcích a systémech umělé inteligence.

Pro výrobce mohou být zapotřebí další povinnosti, které zajistí, že tyto výrobky nebo systémy budou obsahovat prvky, které po dobu své životnosti budou bránit nahrání softwaru s dopadem na jejich bezpečnost.

Vznikající digitální technologie jsou vposled ovlivněny také **složitými hodnotovými řetězci.** Tato složitost však není nová, ani se nejedná výhradně o otázku nově vznikajících digitálních technologií, jako jsou umělá inteligence či internet věcí. Týká se například výrobků, jako jsou počítače, servisní roboti nebo dopravní systémy.

Podle rámce Unie pro bezpečnost výrobků nese odpovědnost za bezpečnost výrobku výrobce, který uvádí výrobek na trh, bez ohledu na to, jak složitý je hodnotový řetězec. Výrobci odpovídají za bezpečnost konečného výrobku, včetně částí, které jsou součástí výrobku, např. softwaru počítače.

Některé právní předpisy Unie týkající se bezpečnosti výrobků již obsahují ustanovení, která výslovně odkazují na situace, v nichž několik hospodářských subjektů zasahuje do daného výrobku před jeho uvedením na trh. Například směrnice o výtazích[54] vyžaduje, aby hospodářský subjekt odpovědný za návrh a výrobu výtahu dal k dispozici osobě odpovědné za instalaci výtahu[55] „*všechny nezbytné dokumenty a informace, aby mohla zajistit správnou a bezpečnou instalaci a vyzkoušení výtahu*.“ Směrnice o strojních zařízeních vyžaduje, aby výrobci zařízení poskytli provozovateli informace o způsobu montáže tohoto zařízení k dalším strojním zařízením[56].

Právní předpisy Unie týkající se bezpečnosti výrobků zohledňují složitost hodnotových řetězců a ukládají povinnosti více hospodářským subjektům na základě zásady „sdílené odpovědnosti“.

I když se odpovědnost výrobce za bezpečnost konečného výrobku ukázala jako dostatečná pro současné složité hodnotové řetězce, právní jistotu i pro případné složitější hodnotové

[52] Rádiové moduly jsou elektronická zařízení, která vysílají a případně přijímají rádiové signály (WIFI, Bluetooth) mezi dvěma zařízeními.

[53] Čl. 3 odst. 3 písm. i) směrnice o rádiových zařízeních.

[54] Podle čl. 16 odst. 2 směrnice 2014/33/EU.

[55] Podle směrnice 2014/33/EU o výtazích zaujímá dodavatel (tedy osoba odpovědná za instalaci) pozici výrobce a musí převzít odpovědnost za návrh, výrobu, instalaci a uvedení výtahu na trh.

[56] Směrnice o strojních zařízeních, příloha I, čl. 1.7.4.2 stanoví, že: *„Každý návod k používání musí obsahovat pokud možno alespoň tyto údaje:“* i) *„pokyny k montáži, instalaci a připojení, včetně nákresů, schémat a prostředků upevnění a označení podstavce nebo zařízení, na něž se má strojní zařízení namontovat;“*

řetězce by mohla poskytnout výslovná ustanovení, která by konkrétně požadovala spolupráci mezi hospodářskými subjekty v dodavatelském řetězci a uživateli. Odpovědnost by tak nesli všichni aktéři v hodnotovém řetězci, kteří mají dopad na bezpečnost výrobků (např. výrobci softwaru) a uživatelé (např. v případě, že výrobek upraví), a dalším aktérům v řetězci by poskytovali nezbytné informace a opatření.

3. Odpovědnost

Na úrovni Unie představují ustanovení o bezpečnosti výrobků a ustanovení o odpovědnosti za výrobky dva vzájemně se doplňující mechanismy, které mají sledovat stejný cíl – fungování jednotného trhu se zbožím, který zajišťuje vysokou úroveň bezpečnosti, tj. minimalizuje riziko újmy pro uživatele a stanoví náhradu škod způsobených vadným zbožím.

Na vnitrostátní úrovni tyto předpisy Unie doplňují neharmonizované rámce pro občanskoprávní odpovědnost, které zajišťují náhradu škod způsobených různými příčinami (např. výrobky a službami) ve vztahu k různým odpovědným osobám (např. vlastníkům, provozovatelům nebo k poskytovatelům služeb).

K nehodám může docházet i navzdory optimalizaci unijních bezpečnostních pravidel v oblasti umělé inteligence, která pomáhá jim předcházet. V takové situaci se jedná o otázku občanskoprávní odpovědnosti. Pravidla občanskoprávní odpovědnosti hrají v naší společnosti dvojí úlohu: na jedné straně zajišťují, aby oběti poškození způsobené jinými osobami získaly náhradu škody, na straně druhé poskytují ekonomickou motivaci pro odpovědnou stranu, aby těmto škodám předcházela. Pravidla o odpovědnosti musí vždy usilovat o rovnováhu mezi ochranou občanů před újmou a usnadněním inovací pro podniky.

Rámce odpovědnosti v Unii fungují dobře. Spoléhají se na souběžné uplatňování směrnice o odpovědnosti za výrobky (směrnice 85/374/EHS), která harmonizovala odpovědnost výrobce vadných výrobků, a dalších neharmonizovaných vnitrostátních režimů odpovědnosti.

Směrnice o odpovědnosti za výrobky poskytuje vrstvu ochrany, kterou vnitrostátní odpovědnost na základě zavinění neposkytuje. Zavádí systém objektivní odpovědnosti výrobce za škodu způsobenou vadou jejich výrobků. V případě újmy na zdraví nebo věcné škody má poškozený nárok na náhradu škody v případě, že prokáže škodu, vadu výrobku (tj. že výrobek neposkytoval takovou úroveň bezpečnosti, jakou má veřejnost právo očekávat) a příčinnou souvislost mezi vadným výrobkem a škodou.

Vnitrostátní neharmonizované režimy stanoví pravidla pro odpovědnost na základě zavinění, podle nichž musí oběti poškození prokázat zavinění osoby odpovědné za škodu, škodu a příčinnou souvislost mezi zaviněním a škodou, aby bylo možné prokázat nárok na náhradu škody. Stanoví rovněž režimy objektivní odpovědnosti, v nichž vnitrostátní zákonodárce přičítá odpovědnost za riziko konkrétní osobě, aniž by bylo nutné, aby oběť prokázala zavinění/vadu nebo příčinnou souvislost mezi zaviněním/vadou a škodou.

Vnitrostátní režimy odpovědnosti poskytují obětem škod způsobených výrobky a službami několik paralelních nároků na odškodnění, a to na základě zavinění nebo objektivní odpovědnosti. Tyto nároky často směřují vůči různým odpovědným osobám a mají různé podmínky.

Například poškozený, který je účastníkem dopravní nehody, má obvykle objektivní nárok vůči majiteli vozidla (tj. osobě, která uzavřela pojištění odpovědnosti z provozu motorových vozidel) a nárok na odpovědnost za škodu založený na zavinění vůči řidiči, oba dva podle

vnitrostátního občanského práva, ale podle směrnice o odpovědnosti za vadné výrobky má nárok i vůči výrobci vozidla, pokud mělo vozidlo vadu.

V souladu s harmonizovanými pravidly o pojištění motorových vozidel musí být používání vozidla pojištěno[57] a prvním kontaktním místem pro uplatnění nároku na náhradu za újmu na zdraví nebo za hmotnou škodu je v praxi vždy pojistitel. Podle těchto pravidel povinné pojištění odškodňuje oběti a chrání pojištěnou osobu, která je podle pravidel vnitrostátního občanského práva[58] odpovědná za finanční náhradu škody způsobené v důsledku nehody motorového vozidla. Na výrobce se podle směrnice o odpovědnosti za vadné výrobky povinné pojištění nevztahuje. Pokud jde o pojištění motorových vozidel, s autonomními vozidly se v právních předpisech Unie zachází stejně jako s těmi neautonomními. Autonomní vozidla, tak jako všechna vozidla, musí být kryta pojištěním odpovědnosti z provozu motorových vozidel třetí strany, které pro poškozenou stranu představuje nejsnazší způsob, jak získat náhradu škody.

Řádné pojištění může zajištěním hladkého odškodnění oběti zmírnit negativní důsledky nehod. Jasná pravidla odpovědnosti pomáhají pojišťovnám vypočítat rizika a požadovat náhradu od strany, která je v konečném důsledku za škodu odpovědná. Například v případě nehody, která je způsobena vadou, může pojistitel po odškodnění oběti požadovat náhradu od výrobce.

Vlastnosti vznikajících digitálních technologií, jako jsou umělá inteligence, internet věcí a robotika, však představují komplikace pro některé aspekty unijních a vnitrostátních rámců odpovědnosti a mohly by snížit jejich účinnost. Některé z těchto vlastností by mohly vést k obtížím při hledání lidského zavinění škody, na jehož základě by bylo možné podle vnitrostátních pravidel vznést nárok na odškodnění založený na zavinění. To znamená, že by prokazování nároku na náhradu škody založeného na vnitrostátních přestupkových předpisech mohlo být obtížné nebo příliš nákladné, což by mohlo vést k tomu, že by oběti nebyly náležitě odškodněny. Je důležité, aby oběti nehod způsobených výrobky a službami využívajícími vznikající digitální technologie, jako je umělá inteligence, neměly v porovnání s jinými podobnými výrobky a službami nižší úroveň ochrany, která vede k náhradě škod podle vnitrostátních přestupkových předpisů. To by mohlo snížit přijetí těchto vznikajících technologií ze strany společnosti a vést k váhání, zda je využívat.

Bude třeba posoudit, zda by komplikace, které nové technologie představují pro stávající rámce, mohly rovněž způsobit právní nejistotu, pokud jde o uplatňování stávajících právních předpisů (např. jak by se pojem „zavinění“ vztahoval na škody způsobené umělou inteligencí). Ty by totiž mohly odrazovat investice a zvyšovat náklady na informace a pojištění pro výrobce a další podniky v dodavatelském řetězci, zejména pak pro evropské malé a střední podniky. Navíc pokud by nakonec členské státy řešily tyto komplikace ve vnitrostátních rámcích odpovědnosti, mohlo by to vést k další fragmentaci, čímž by se zvýšily náklady na zavádění inovativních řešení v oblasti umělé inteligence a snížil přeshraniční obchod na jednotném trhu. Je důležité, aby společnosti znaly svá rizika spojená s odpovědností v celém hodnotovém řetězci a mohly je snižovat nebo jim zabránit a účinně se proti těmto rizikům pojistit.

[57] Harmonizovaná pravidla pro motorová vozidla týkající se pojištění odpovědnosti z provozu motorových vozidel a kontrole povinnosti uzavřít takové pojištění odpovědnosti podle směrnice 2009/103/ES.

[58] Ve většině členských států se objektivní odpovědnost vztahuje na osobu, na jejíž jméno je motorové vozidlo registrováno.

Tato kapitola vysvětluje, jaké výzvy nové technologie představují pro stávající rámce a jakým způsobem lze tyto výzvy řešit. Hlubší úvahu si dále zasluhují zvláštní rysy některých odvětví, například zdravotní péče.

Složitost výrobků, služeb a hodnotového řetězce: Technologie a průmysl se v posledních desetiletích výrazně rozvíjejí. Zejména dělicí čára mezi výrobky a službami není vždy tak jednoznačná, jak bývala dřív. Provázanost mezi výrobky a poskytováním služeb je čím dál hlubší. Ačkoli složité výrobky a hodnotové řetězce nejsou pro evropský průmysl a jeho regulační model ničím novým, co se týče odpovědnosti za výrobky, zasluhují si software a umělá inteligence zvláštní pozornost. Software má zásadní význam pro fungování mnoha výrobků a může mít vliv na jejich bezpečnost. Je integrován do výrobků, ale může být rovněž dodáván odděleně, aby bylo umožněno použití výrobku tak, jak je zamýšleno. Použitelnost počítačů a chytrých telefonů bez softwaru není obzvlášť vysoká. To znamená, že software může způsobit vadu konkrétního výrobku a vést k hmotným škodám (viz rámeček o softwaru v části týkající se bezpečnosti). To by případně mohlo vést k odpovědnosti výrobce výrobku podle směrnice o odpovědnosti za vadné výrobky.

Vzhledem k tomu, že existuje mnoho druhů software, klasifikace softwaru jako služby nebo jako výrobku nemusí být vždy snadná. I pokud by se software, který ovládá funkce hmotného výrobku, dal považovat za konstrukční část nebo součást tohoto výrobku, klasifikace některých forem samostatného softwaru by mohla být obtížnější.

Ačkoli definice výrobku podle směrnice o odpovědnosti za výrobky je široká, její rozsah by mohl být dále objasněn, aby lépe odrážel složitost vznikajících technologií a aby vždy zajistil dostupnost náhrady škod způsobených výrobky, které jsou vadné po stránce softwaru nebo jiných digitálních prvků. To by hospodářským subjektům, jako jsou vývojáři softwaru, umožnilo lépe posoudit, zda by mohli být podle směrnice o odpovědnosti za výrobky považováni za výrobce.

Aplikace umělé inteligence jsou často integrovány do **složitých prostředí internetu věcí**, kde dochází k interakci mnoha různých propojených zařízení a služeb. Kombinace různých digitálních složek ve složitém ekosystému a množství zúčastněných aktérů může vést k tomu, že je obtížné posoudit, kde leží příčina potenciální škody a kdo je za ni odpovědný. Vzhledem ke složitosti těchto technologií může být pro oběti velmi obtížné určit odpovědnou osobu a prokázat všechny nezbytné podmínky pro úspěšné uplatnění nároku v souladu s požadavky vnitrostátního práva. Náklady na tyto odborné znalosti mohou být ekonomicky neúnosné a mohou odrazovat oběti od uplatňování nároku na odškodnění.

Kromě toho budou výrobky a služby založené na umělé inteligenci interagovat s tradičními technologiemi, což dále zvýší úroveň složitosti v oblasti odpovědnosti. Například autonomní vozidla budou po určitou dobu sdílet silnici s těmi tradičními. V některých odvětvích služeb (např. řízení dopravy a zdravotní péče), kde budou částečně automatizované systémy umělé inteligence podporovat lidské rozhodování, bude existovat podobná složitost.

Podle zprávy[59] sestavy pro nové technologie v rámci skupiny odborníků pro odpovědnost a nové technologie lze zvážit úpravy vnitrostátních právních předpisů za účelem usnadnění důkazního břemene pro oběti škod vzniklých v souvislosti s umělou inteligencí. Například důkazní břemeno by mohlo být spojeno s vyhověním (příslušným provozovatelem) požadavkům na kybernetickou bezpečnost nebo jiným povinnostem v oblasti bezpečnosti

[59] Odpovědnost za umělou inteligenci a další nové digitální technologie, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

stanovenými zákonem: pokud těmto pravidlům není vyhověno, bylo by možné změnit důkazní břemeno, pokud jde o zavinění a příčinnou souvislost.

Komise sbírá názory na to, zda a do jaké míry může být zapotřebí zmírnit důsledky složitosti tím, že by se v případě škod způsobených provozem aplikací s umělou inteligencí prostřednictvím vhodné iniciativy EU zmírnilo nebo obrátilo důkazní břemeno vyžadované vnitrostátními předpisy o odpovědnosti.

Pokud jde o právní předpisy Unie, podle směrnice o odpovědnosti za vadné výrobky by byl výrobek, který nesplňuje závazná bezpečnostní pravidla, považován za vadný, a to bez ohledu na zavinění výrobce. Rovněž však může být přínosné zvážit způsoby, jak usnadnit důkazní břemeno pro oběti podle uvedené směrnice: směrnice se opírá o vnitrostátní pravidla týkající se důkazů a zjištění příčinné souvislosti.

Propojenost a otevřenost: V současné době není zcela jasné, jaká mají být bezpečnostní očekávání ohledně škod vyplývajících z narušení kybernetické bezpečnosti výrobku a zda by tyto škody byly podle směrnice o odpovědnosti za vadné výrobky odpovídajícím způsobem nahrazeny.

Nedostatky v kybernetické bezpečnosti mohou existovat od počátečního uvedení výrobku do oběhu, ale mohou se objevit i později, dlouho poté, co byl výrobek uveden do oběhu.

V rámci odpovědnosti vyplývající ze zavinění umožní stanovení jasných povinností v oblasti kybernetické bezpečnosti provozovatelům určit, co musí udělat, aby se vyhnuli následkům odpovědnosti.

Podle směrnice o odpovědnosti za výrobky by se mohla otázka, zda by výrobce mohl předvídat některé změny s ohledem na rozumně předvídatelné použití výrobku, dostat do popředí. Je například možné, že dojde ke zvýšenému používání strategie „odvolávání se na vadu, která nastala později“, podle níž výrobce není odpovědný v případě, kdy vada neexistovala v okamžiku uvedení výrobku do oběhu, nebo strategie „odvolávání se vývojové riziko“ (totiž že stav vědeckých a technických znalostí v době, kdy byl výrobek uveden na trh, neumožnil zjistit jeho vadu). Odpovědnost by navíc mohla být snížena, pokud poškozená strana neprovádí příslušné bezpečnostní aktualizace. To by mohlo být potenciálně považováno za spoluzavinění ze strany poškozené osoby, a snížit tak odpovědnost výrobce. S tím, jak se se pojem předpokládaného rozumného užívání a otázky spoluzavinění z nedbalosti, například nestáhnutím bezpečnostní aktualizace, zřejmě budou objevovat častěji, může být pro poškozené osoby obtížnější získat náhradu škody způsobené vadou výrobku.

Autonomie a neprůhlednost: Pokud jsou aplikace umělé inteligence schopny jednat samostatně, plní úkoly, aniž by byl každý krok předem definován, s nižší mírou lidské kontroly či dohledu, či zcela bez kontroly a dohledu. Algoritmy založené na strojovém učení může být obtížné, ne-li nemožné, pochopit (tzv. efekt černé skříňky).

Kromě složitosti, o níž se pojednává výše, by se v důsledku tohoto efektu černé skříňky u některých umělých inteligencí mohlo dosažení náhrady škody způsobené autonomními aplikacemi s umělou inteligencí zkomplikovat. Potřeba porozumět algoritmu a datům, která umělá inteligence používá, vyžaduje analytické kapacity a technické odborné znalosti, které by pro oběti mohly být příliš nákladné. Přístup k algoritmu a údajům by navíc mohl být bez spolupráce potenciálně odpovědné strany nemožný. V praxi by tak pro oběti mohlo být uplatnění nároku na náhradu škody nemožné. Kromě toho by nebylo jasné, jak prokázat zavinění umělé inteligence jednající samostatně nebo co považovat za pochybení osoby, která se na umělou inteligenci spoléhá.

Vnitrostátní právní předpisy již vypracovaly řadu řešení s cílem snížit důkazní břemeno pro oběti v podobných situacích.

Hlavní zásadou v Unii ohledně bezpečnosti výrobků a odpovědnosti za výrobky je i nadále to, že je povinností výrobce, aby zajistil, že všechny výrobky uvedené na trh budou bezpečné během celého svého životního cyklu a rovněž při svém používání, které lze rozumně očekávat. To znamená, že výrobce by musel zajistit, aby výrobek používající umělou inteligenci respektoval určité bezpečnostní parametry. Vlastnosti umělé inteligence nevylučují možnost očekávat od výrobků, že budou bezpečné, ať se jedná o automatické sekačky na trávu nebo o chirurgické roboty.

Autonomie může bezpečnost výrobku ovlivnit, neboť může podstatně změnit vlastnosti výrobku, včetně jeho bezpečnostních prvků. Je otázkou, za jakých podmínek vlastnosti samostatného učení prodlužují odpovědnost výrobce a v jakém rozsahu by měl výrobce předvídat určité změny.

V úzké koordinaci s odpovídajícími změnami v bezpečnostním rámci Unie by mohl být přehodnocen pojem „uvedení do oběhu“, který je v současné době používán směrnicí o odpovědnosti za výrobky, tak, aby se zohlednilo, že se výrobky mohou měnit a že mohou být upravovány. To by rovněž mohlo pomoci vyjasnit, kdo je odpovědný za veškeré změny na výrobku.

Podle zprávy[60] sestavy pro nové technologie v rámci skupiny odborníků pro odpovědnost a nové technologie by provoz některých autonomních zařízení a služeb využívajících umělou inteligenci mohl mít z hlediska odpovědnosti specifický rizikový profil, protože mohou způsobit značnou újmu na důležitých právních zájmech, jako jsou život, zdraví a majetek, a vystavit veřejnost rizikům. To by se mohlo týkat zejména zařízení s umělou inteligencí, která se pohybují ve veřejných prostorách (např. plně autonomní vozidla, drony[61] a roboti doručující balíky), nebo služeb založených na umělé inteligenci s podobnými riziky (např. služby řízení dopravy, navádění nebo ovládání vozidel, či řízení distribuce energie). Výzvy, které pro vnitrostátní přestupkové předpisy představují autonomie a neprůhlednost, by mohly být řešeny pomocí přístupu založeného na posouzení rizik. To, aby v případě vzniku tohoto rizika byla oběť odškodněna bez ohledu na zavinění, by mohly zajistit režimy objektivní odpovědnosti. Bylo by třeba pečlivě posoudit dopad, jaký bude mít na vývoj a zavádění umělé inteligence volba strany, která bude za jejich provoz objektivně odpovědná, a zvážit přístup na základě posouzení rizik.

U provozu aplikací umělé inteligence se zvláštním rizikovým profilem se Komise sbírá názory na to, zda a do jaké míry může být za účelem dosažení účinné náhrady pro případné oběti nutná objektivní odpovědnost, jak je stanovena ve vnitrostátních právních předpisech pro podobná rizika, kterým je veřejnost vystavena (například u provozu motorových vozidel, letadel nebo jaderných elektráren). Aby byla náhrada škod zajištěna bez ohledu na solventnost odpovědné osoby a aby byly sníženy náklady škody, sbírá Komise rovněž názory k možnosti kombinovat objektivní odpovědnost s možnou povinností uzavřít dostupné pojištění podle vzoru směrnice o pojištění motorových vozidel.

[60] Odpovědnost za umělou inteligenci a další nové digitální technologie, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

[61] Srov. bezpilotní systémy uvedené v prováděcím nařízení Komise (EU) 2019/947 ze dne 24. května 2019 o pravidlech a postupech pro provoz bezpilotních letadel.

Pokud jde o provoz všech ostatních aplikací umělé inteligence, což by byla převážná většina takových aplikací, uvažuje Komise nad tím, zda je třeba přizpůsobit důkazní břemeno týkající se příčin a zavinění. V tomto ohledu je jedním z problémů uvedených ve zprávě[62] sestavy pro nové technologie v rámci skupiny odborníků pro odpovědnost a nové technologie situace, kdy potenciálně odpovědná strana nezaznamenala údaje relevantní pro posouzení odpovědnosti nebo je není ochotna s obětí sdílet.

4. Závěr

Vznik nových digitálních technologií, jako jsou umělá inteligence, internet věcí a robotika, přináší v oblastech bezpečnosti výrobků a odpovědnosti nové výzvy, jako jsou konektivita, autonomie, závislost na datech, neprůhlednost, složitost výrobků a systémů, aktualizace softwaru a složitější řízení bezpečnosti a hodnotové řetězce.

Stávající právní předpisy v oblasti bezpečnosti výrobků obsahují řadu nedostatků, které je třeba řešit, zejména úpravami směrnice o obecné bezpečnosti výrobků, směrnice o strojních zařízeních, směrnice o rádiových zařízeních a nového legislativního rámce. Práce na přizpůsobení různých právních předpisů v tomto rámci bude v budoucnu probíhat jednotným a harmonizovaným způsobem.

Nové výzvy v otázkách bezpečnosti představují rovněž nové výzvy v otázkách odpovědnosti. Tyto výzvy spojené s odpovědností je třeba řešit, aby byla zajištěna stejná úroveň ochrany ve srovnání s tou, která existuje pro oběti u tradičních technologií, a to při současném zachování rovnováhy s potřebami technologické inovace. To pomůže vytvářet důvěru v tyto nově vznikající digitální technologie a vytvoří investiční stabilitu.

I když jsou stávající právní předpisy Unie a členských států v zásadě schopné udržet se vznikajícími technologiemi krok, rozměr a kombinovaný účinek výzev v oblasti umělé inteligence by mohl v některých oprávněných případech komplikovat odškodnění obětí[63]. V důsledku toho může být v případě škody rozdělení nákladů podle stávajících pravidel nepřiměřené nebo neúčinné. Aby byla tato situace napravena a případné nejistoty ve stávajícím rámci vyřešeny, lze zvážit určité úpravy směrnice o odpovědnosti za výrobky a vnitrostátních režimů odpovědnosti prostřednictvím vhodných iniciativ EU založených na cíleném posouzení rizik, tj. s přihlédnutím k tomu, že různé aplikace s umělou inteligencí představují různá rizika.

[62] Odpovědnost za umělou inteligenci a další nové digitální technologie, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

[63] Viz zpráva sestavy pro nové technologie, s. 3, a doporučení 27.2. odborné skupiny na vysoké úrovni pro umělou inteligenci.