EVROPSKÁ
KOMISE

V Bruselu dne 19.2.2020
COM(2020) 65 final

BÍLÁ KNIHA

o umělé inteligenci - evropský přístup k excelenci a důvěře

Bílá kniha o umělé inteligenci: evropský přístup k excelenci a důvěře

Umělá inteligence je na vzestupu. Bude měnit náš život zlepšováním zdravotní péče (umožní např. stanovení přesnější diagnózy či lepší prevenci nemocí), zvyšováním účinnosti zemědělství, přispíváním ke zmírňování změny klimatu a přizpůsobování se této změně, zlepšováním účinnosti výrobních systémů prostřednictvím prediktivní údržby, zvyšováním bezpečnosti Evropanů a mnoha jinými způsoby, které si zatím umíme představit pouze v náznacích. Umělá inteligence zároveň zahrnuje řadu potenciálních rizik, jako je netransparentní rozhodování, diskriminace na základě pohlaví nebo jiné druhy diskriminace, narušování našeho soukromí nebo může být zneužita k páchání trestné činnosti.

S ohledem na silnou celosvětovou konkurenci je zapotřebí jednotný evropský přístup, který bude vycházet z evropské strategie pro umělou inteligenci, která byla představena v dubnu 2018[1]. Aby EU mohla reagovat na příležitosti a problémy spojené s umělou inteligencí, musí při podpoře rozvoje a zavádění umělé inteligence jednat jako jeden celek a definovat svou vlastní cestu založenou na evropských hodnotách.

Komise je odhodlána vytvořit podmínky pro vědecký průlom, zachovat vedoucí postavení EU v oblasti technologií a zajistit, aby nové technologie byly ve službách všech Evropanů – a zlepšily tak jejich život, přičemž musí být respektována jejich práva.

Předsedkyně Komise Ursula von der Leyenová ve svých politických směrech[2] nastínila koordinovaný evropský přístup k lidským a etickým důsledkům umělé inteligence a uvedla rovněž, že je třeba lépe využívat data velkého objemu pro inovace.

Komise proto podporuje přístup zaměřený na regulaci a investice s dvojím cílem: podporovat zavádění umělé inteligence a zabývat se riziky spojenými s některými způsoby využití této nové technologie. Účelem této bílé knihy je nastínit politické možnosti k dosažení těchto cílů. Nezabývá se vývojem a používáním umělé inteligence pro vojenské účely. Komise vyzývá členské státy, ostatní evropské orgány a všechny zúčastněné strany, včetně průmyslu, sociálních partnerů, organizací občanské společnosti, výzkumných pracovníků, veřejnost obecně a jakékoli zainteresované strany, aby reagovaly na níže popsané možnosti a přispěly k budoucímu rozhodování Komise v této oblasti.

1. ÚVOD

Vzhledem k tomu, že se digitální technologie stávají stále důležitější součástí všech oblastí každodenního života, je nutné, aby jim občané mohli důvěřovat. Důvěryhodnost je rovněž předpokladem pro jejich zavádění. Je to příležitost pro Evropu, jednak vzhledem k tomu, že je odhodlána hájit pevně své hodnoty a zásady právního státu, a jednak, že je prokazatelně schopna produkovat bezpečné, spolehlivé sofistikované výrobky a služby od letectví přes energetiku, až po automobilové a zdravotnické vybavení.

Současný a budoucí udržitelný hospodářský růst a společenský blahobyt Evropy stále více závisí na hodnotě, kterou představují data. Umělá inteligence je jednou z nejdůležitějších aplikací ekonomiky založené na datech. V současnosti se většina dat týká spotřebitelů a je uchovávána a zpracovávána v

[1] Umělá inteligence pro Evropu, COM/2018/237 final

[2] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_cs.pdf.

centrální cloudové infrastruktuře. Naopak v budoucnu bude mnohem větší část rozsáhlého objemu dat pocházet z průmyslu, podniků a veřejného sektoru a bude uložena v různých systémech, zejména na výpočetních zařízeních fungujících na okraji sítě (*at the edge*). Evropě, která má silné postavení v digitalizovaném průmyslu i v rámci mezipodnikových aplikací, avšak poměrně zaostává v oblasti spotřebitelských platforem, se tak otevírají nové příležitosti.

Jednoduše řečeno, umělá inteligence je soubor technologií, které kombinují data, algoritmy a výpočetní výkon. Pokrok v oblasti výpočetní techniky a rostoucí dostupnost údajů jsou proto klíčovými faktory současného rychlého rozvoje umělé inteligence. Evropa může spojit své silné stránky v oblasti technologií a průmyslu s vysoce kvalitní digitální infrastrukturou a regulačním rámcem založeným na základních evropských hodnotách, aby se **stala světovým lídrem inovací v ekonomice založené na datech a jejích aplikacích**, jak je stanoveno v evropské strategii pro data[3]. Na základě toho může vytvořit ekosystém umělé inteligence, který přinese užitek celé evropské společnosti a ekonomice:

- **občanům**, aby mohli využívat nových přínosů, například lepší zdravotní péče, menší poruchovosti zařízení v domácnosti, bezpečnějších a čistších dopravních systémů a lepších veřejných služeb,
- pro rozvoj **podniků**, které vyvíjejí například novou generaci produktů a služeb v oblastech, v nichž je Evropa obzvláště silná (strojírenství, doprava, kybernetická bezpečnost, zemědělství, ekologické a oběhové hospodářství, zdravotní péče a odvětví s vysokou přidanou hodnotou, jako je móda a cestovní ruch), a
- pro služby **veřejného zájmu**, například snížením nákladů na poskytování služeb (dopravu, vzdělávání, energetiku a nakládání s odpady), zlepšováním udržitelnosti produktů [4] a poskytnutím vhodných nástrojů donucovacím orgánům k zajištění bezpečnosti občanů [5] s náležitými zárukami, pokud jde o dodržování jejich práv a svobod.

Vzhledem k velkému vlivu umělé inteligence na naši společnost a nutnosti vybudovat důvěru, je zásadně důležité, aby evropská umělá inteligence byla založena na našich hodnotách a základních právech, jako je lidská důstojnost a ochrana soukromí.

Dopady systémů umělé inteligence by se dále neměly posuzovat jen z pohledu jednotlivce, ale také z hlediska společnosti jako celku. Používání systémů umělé inteligence může hrát významnou úlohu při plnění cílů udržitelného rozvoje a podpoře demokratických procesů a sociálních práv. Evropa se svými nedávnými návrhy týkajícími se Zelené dohody pro Evropu[6] stojí v čele řešení problémů spojených s klimatem a životním prostředím. Digitální technologie, jako je umělá inteligence, jsou rozhodujícím faktorem pro dosažení cílů Zelená dohody pro Evropu. Vzhledem k rostoucímu významu umělé inteligence musí být dopad systémů umělé inteligence na životní prostředí náležitě zohledněn v

[3] COM(2020) 66 final.

[4] Umělá inteligence a digitalizace jsou zásadním předpokladem k dosažení cílů Zelené dohody pro Evropu. Současná environmentální stopa odvětví IKT však podle odhadů představuje více než 2 % všech celosvětových emisí. Evropská digitální strategie, která je připojena k této bílé knize, obsahuje návrhy opatření pro zelenou transformaci digitálního odvětví.

[5] Nástroje umělé inteligence mohou poskytnout možnosti pro lepší ochranu občanů EU před trestnou činností a teroristickými činy.

Tyto nástroje by například mohly pomoci identifikovat teroristickou propagandu na internetu, odhalit podezřelé transakce při prodeji nebezpečných výrobků, identifikovat nebezpečné skryté předměty nebo nedovolené látky či produkty, nabídnout pomoc občanům v krizových situacích a pomoci poskytovat pokyny zásahovým složkám.

[6] COM(2019) 640 final.

průběhu jejich životního cyklu a v rámci celého dodavatelského řetězce, např. pokud jde o využívání zdrojů pro učení algoritmů a ukládání dat.

Společný evropský přístup k umělé inteligenci je nezbytný pro dosažení dostatečného rozsahu a zabránění roztříštěnosti jednotného trhu. Zavedení vnitrostátních iniciativ může ohrozit právní jistotu, oslabit důvěru občanů a zabránit vzniku dynamického evropského průmyslu.

V této bílé knize jsou představeny možnosti politiky, které umožní důvěryhodný a bezpečný rozvoj umělé inteligence v Evropě, přičemž budou plně respektovány hodnoty a práva občanů EU. Hlavními stavebními kameny této bílé knihy jsou:

- Politický rámec, který stanoví opatření pro sladění úsilí na evropské, vnitrostátní a regionální úrovni. Cílem rámce je za spolupráce soukromého a veřejného sektoru mobilizovat zdroje k dosažení **„ekosystému excelence“** v celém hodnotovém řetězci, počínaje výzkumem a inovacemi, a vytvořit správné pobídky k rychlejšímu přijímání řešení založených na umělé inteligenci, a to i v malých a středních podnicích.
- Klíčové prvky budoucího regulačního rámce pro umělou inteligenci v Evropě, který vytvoří jedinečný **„ekosystém důvěry“**. Za tím účelem je nutné zajistit soulad s pravidly EU, včetně pravidel na ochranu základních práv a práv spotřebitelů, zejména pokud jde o systémy umělé inteligence provozované v EU, které představují vysoké riziko[7]. Vytvoření ekosystému důvěry je samo o sobě politickým cílem a mělo by občanům poskytnout důvěru v zavádění aplikací umělé inteligence a podnikům a veřejným organizacím právní jistotu pro inovace zahrnující umělou inteligenci. Komise důrazně podporuje přístup zaměřený na člověka, který vychází ze sdělení o budování důvěry v umělou inteligenci zaměřenou na člověka[8], a rovněž zohlední poznatky získané během pilotní fáze etických pokynů, které vypracovala odborná skupina na vysoké úrovni pro umělou inteligenci.

Cílem evropské strategie pro data, která je přiložena k této bílé knize, je umožnit Evropě stát se nejatraktivnější, nejbezpečnější a nejdynamičtější ekonomikou na světě založenou na pružném využívání dat – a umožnit tak Evropě díky orientaci na data zlepšit své rozhodování a každodenní život všech občanů. Strategie stanoví řadu politických opatření, včetně mobilizace soukromých a veřejných investic potřebných pro dosažení tohoto cíle. Jaké důsledky bude mít umělá inteligence, internet věcí a další digitální technologie pro právní předpisy v oblasti bezpečnosti a odpovědnosti, analyzuje zpráva Komise připojená k této bílé knize.

2. VYUŽITÍ SILNÝCH STRÁNEK NA PRŮMYSLOVÝCH A PROFESNÍCH TRZÍCH

Evropa má dobré předpoklady k tomu, aby využila potenciál umělé inteligence, a to nejen jako uživatel, ale také jako tvůrce a výrobce této technologie. Disponuje špičkovými výzkumnými centry, inovativními startupy, má přední pozici na světě v robotice a konkurenceschopných odvětvích výroby a služeb, od automobilového průmyslu přes zdravotní péči, energetiku, finanční služby, až po zemědělství. Evropa vyvinula silnou výpočetní infrastrukturu (např. vysoce výkonné počítače), která je pro fungování umělé inteligence klíčová. Evropa rovněž disponuje velkými objemy veřejných a průmyslových dat, jejichž potenciál v současnosti není dostatečně využit. Je uznávána za své silné průmyslové stránky, např. bezpečné a zabezpečené digitální systémy s nízkou spotřebou energie, které jsou pro další rozvoj umělé inteligence zásadní.

[7] Je možné, že bude nutné zavést další opatření pro předcházení zneužívání umělé inteligence pro trestnou činnost a pro boj proti této trestné činnosti, tato problematika je však mimo oblast působnosti této bílé knihy.
[8] COM (2019) 168.

Využití schopnosti EU investovat do technologií a infrastruktur příští generace, jakož i do digitálních kompetencí, jako je datová gramotnost, zvýší technologickou suverenitu Evropy v klíčových technologiích a infrastrukturách, které jsou předpokladem pro další rozvoj ekonomiky založené na datech. Tyto infrastruktury by měly podporovat vytváření evropských datových poolů, které jsou předpokladem důvěryhodné umělé inteligence, tj. umělé inteligence založené na evropských hodnotách a pravidlech.

Evropa by měla využít své přednosti k posílení svého postavení v těchto ekosystémech a v celém hodnotovém řetězci, od výroby hardwaru přes software až po odvětví služeb. To se již do určité míry daří. Evropa produkuje více než čtvrtinu průmyslových a profesionálních robotů pro oblast služeb (např. pro přesné zemědělství, bezpečnost, zdravotnictví a logistiku) a hraje důležitou úlohu ve vývoji a využívání softwarových aplikací pro podniky a organizace (mezipodnikové aplikace (B2B), jako je plánování podnikových zdrojů, konstrukční a inženýrský software), jakož i aplikací na podporu elektronické veřejné správy a „inteligentních podniků“.

Evropa má vedoucí pozici v zavádění umělé inteligence do výroby. Více než polovina předních evropských výrobců zavádí umělou inteligenci alespoň v jednom kroku výrobních operací[9].

Jedním z důvodů silného postavení Evropy v oblasti výzkumu je program financování EU, který se ukázal být velmi účinný pro sdružování úsilí, předcházení zdvojování snah a zvyšování veřejných a soukromých investic v členských státech. V posledních třech letech finanční prostředky EU na výzkum a inovace v oblasti umělé inteligence vzrostly na 1,5 miliardy EUR, což ve srovnání s předchozím obdobím představuje nárůst o 70 %.

Investice do výzkumu a inovací v Evropě však stále představují pouze zlomek veřejných a soukromých investic, které směřují do této oblasti v jiných regionech světa. V roce 2016 bylo v Evropě do umělé inteligence investováno přibližně 3,2 miliardy EUR, v Severní Americe to pro srovnání bylo přibližně 12,1 miliardy EUR a v Asii 6,5 miliardy EUR[10]. Evropa by měla reagovat a úroveň investic výrazně zvýšit. Koordinovaný plán v oblasti umělé inteligence[11] vytvořený spolu s členskými státy se ukazuje jako dobrý výchozí bod při budování užší spolupráce v oblasti umělé inteligence v Evropě a pro vytváření synergií ve snaze maximalizovat investice do hodnotového řetězce umělé inteligence.

3. VYUŽITÍ VZNIKAJÍCÍCH PŘÍLEŽITOSTÍ: DALŠÍ VLNA DAT

Ačkoli Evropa v současné době nemá silnou pozici v oblasti spotřebitelských aplikací a on-line platforem, což vede ke konkurenčnímu znevýhodnění v přístupu k datům, dochází k významným posunům, pokud jde o hodnotu dat a jejich opětovné využívání ve všech odvětvích. Objem dat produkovaných na světě rychle roste, a to z 33 zettabytů v roce 2018 na očekávaných 175 zettabytů v roce 2025.[12] Každá nová vlna dat je pro Evropu příležitostí k tomu, aby se mohla zapojit do ekonomiky založené na využívání dat a aby se stala světovou jedničkou v této oblasti. Kromě toho se v nadcházejících pěti letech dramaticky změní způsob, jakým se data uchovávají a zpracovávají. V současnosti se zpracování a analýza dat, které probíhají v cloudu, z 80 % provádí v datových centrech a v centralizovaných výpočetních zařízeních a 20 % v inteligentních propojených předmětech, jako

[9] ...Následuje Japonsko (30 %) a USA (28 %). Zdroj: CapGemini (2019).
[10] 10 požadavků na Evropu ve věku umělé inteligence a automatizace, McKinsey, 2017.
[11] COM (2018) 795.
[12] IDC (2019).

jsou automobily, domácí spotřebiče nebo výrobní roboti, a ve výpočetních zařízeních v blízkosti uživatele („*edge computing*“). Do roku 2025 se tento poměr výrazně změní[13].

Evropa je celosvětovým lídrem v oblasti elektroniky s nízkou spotřebou energie, což je klíčové pro příští generaci specializovaných procesorů pro umělou inteligenci. Na tomto trhu v současné době dominují subjekty ze zemí mimo EU, což by se mohlo změnit pomocí iniciativ, jako je evropská iniciativa pro procesory, která se zaměřuje jak na vývoj počítačových systémů s nízkou spotřebou jak pro fungování na okraji sítě, tak pro další generaci vysoce výkonné výpočetní techniky, i na práci společného podniku pro klíčové digitální technologie, který má podle na návrhu zahájit svou činnost v roce 2021. Evropa rovněž vede v oblasti neuromorfních řešení[14], která jsou velmi vhodná pro automatizaci průmyslových procesů (průmysl 4.0) a druhů dopravy a mohou několikanásobně zvýšit energetickou účinnost.

Nedávné pokroky v kvantové výpočetní technice povedou k exponenciálnímu nárůstu kapacity zpracování[15]. Evropa může být v této technologii na předním místě díky akademické vyspělosti v oblasti kvantové výpočetní techniky i silnému postavení evropského průmyslu, pokud jde o kvantové simulátory a programovací prostředí pro kvantovou výpočetní techniku. Evropské iniciativy, jejichž cílem je zvýšit dostupnost kvantových zkušebních a experimentálních zařízení, pomohou přispět k využívání těchto nových kvantových řešení v řadě průmyslových a akademických odvětví.

Evropa bude zároveň i nadále v čele pokroku v algoritmických základech umělé inteligence, přičemž bude vycházet z vlastní vědecké excelence. Je třeba budovat mosty mezi obory, které v současné době nejsou propojeny, jako je strojové učení a hluboké učení (pro něž je příznačná omezená možnost interpretace, potřeba velkého objemu dat pro přípravu modelů a učení prostřednictvím korelací) a symbolické přístupy (kde jsou pravidla vytvářena formou lidského zásahu). Kombinace symbolického uvažování a hlubokých neuronových sítí může pomoci zlepšit vysvětlitelnost výsledků umělé inteligence.

4. EKOSYSTÉM EXCELENCE

K vytvoření ekosystému excelence, který může podpořit rozvoj a využívání umělé inteligence v celém hospodářství EU a veřejné správě, je třeba pokročit na několika úrovních.

A. SPOLUPRÁCE S ČLENSKÝMI STÁTY

Komise v prosinci 2018 představila koordinovaný plán na podporu vývoje a využití umělé inteligence v Evropě[16], který vypracovala společně s členskými státy a který vychází ze strategie pro rozvoj umělé inteligence přijaté v dubnu 2018[17].

Tento plán navrhuje přibližně 70 společných opatření pro užší a účinnější spolupráci mezi členskými státy a Komisí v klíčových oblastech, jako je výzkum, investice, zavádění na trh, dovednosti a talent, data a mezinárodní spolupráce. Plán poběží do roku 2027 a bude pravidelně monitorován a podrobován přezkumu.

---

[13] Gartner (2017).

[14] Neuromorfní řešení je jakýkoli velmi rozsáhlý systém integrovaných obvodů, který napodobuje neurobiologické struktury, které se vyskytují v nervovém systému.

[15] Kvantové počítače budou mít schopnost zpracovat za méně než několik vteřin mnohem objemnější soubory dat než dnešní nejvýkonnější počítače, což umožní vývoj nových aplikací umělé inteligence ve všech odvětvích.

[16] Koordinovaný plán v oblasti umělé inteligence, COM (2018) 795.

[17] Umělá inteligence pro Evropu, COM (2018) 237.

Cílem je maximalizovat dopad investic na výzkum, inovace a zavádění umělé inteligence, posoudit vnitrostátní strategie pro umělou inteligenci a navázat na koordinovaný plán v této oblasti a rozšířit jej s členskými státy:

- *Opatření č. 1: Komise s přihlédnutím k výsledkům veřejné konzultace k bílé knize navrhne členským státům revizi koordinovaného plánu, která má být přijata do konce roku 2020.*

Financování umělé inteligence na úrovni EU by mělo přilákat a soustřeďovat investice do oblastí, ve kterých jsou požadována opatření přesahující rámec toho, čeho mohou jednotlivé členské státy samy dosáhnout. Cílem je získat v příštím desetiletí v EU investice do umělé inteligence v celkové výši přesahující 20 miliard EUR[18] ročně. EU pro mobilizaci soukromých a veřejných investic zpřístupní zdroje z programu Digitální Evropa, programu Horizont Evropa a také z evropských strukturálních a investičních fondů na zohlednění potřeb méně rozvinutých regionů a venkovských oblastí.

Koordinovaný plán by se mohl rovněž zaměřit na společenský a environmentální prospěch jako klíčovou zásadu pro umělou inteligenci. Systémy umělé inteligence jsou příslibem pomoci při řešení nejnaléhavějších problémů, včetně změny klimatu a zhoršování životního prostředí. Je také důležité, aby k tomu docházelo způsobem šetrným k životnímu prostředí. Umělá inteligence může a měla by sama o sobě kriticky zkoumat využívání zdrojů a spotřebu energie a měla by být trénována tak, aby volila rozhodnutí, která jsou pozitivní pro životní prostředí. Komise zváží možnosti, jak společně s členskými státy podpořit a prosazovat odpovídající řešení v oblasti umělé inteligence.

B. ZAMĚŘENÍ ÚSILÍ VÝZKUMNÉ A INOVAČNÍ KOMUNITY

Evropa si nemůže dovolit zachovat současnou roztříštěnost fungování center kompetencí, kdy žádné z nich samostatně nedosáhlo takového rozsahu, aby mohlo soutěžit s předními instituty v celosvětovém měřítku. Je nezbytné vytvořit více synergií a sítě mezi četnými evropskými výzkumnými středisky v oblasti umělé inteligence a sladit jejich úsilí s cílem dosáhnout špičkové úrovně, přilákat nejlepší výzkumné pracovníky a udržet je a rozvíjet nejlepší technologie. Evropa potřebuje průkopnické centrum výzkumu, inovací a odborných znalostí, které by tyto snahy koordinovalo, bylo celosvětovým referenčním standardem v oblasti umělé inteligence, a které by mohlo přilákat investice a největší talenty v tomto oboru.

Centra a sítě by se měly zaměřit na odvětví, v nichž má Evropa potenciál stát se globálním šampionem, jako je průmysl, zdravotnictví, doprava, finance, zemědělsko-potravinářské hodnotové řetězce, energetika/životní prostředí, lesnictví, pozorování Země a vesmír. Ve všech těchto oblastech se Evropa snaží být v čele a nabízí značný potenciál, znalosti a odbornost[19]. Stejně důležité je vytvořit testovací a experimentační zařízení na podporu rozvoje a následného zavádění nových aplikací umělé inteligence.

- *Opatření č. 2: Komise usnadní vytvoření center excelence a testovacích center, která mohou kombinovat evropské, vnitrostátní a soukromé investice, případně i nový právní nástroj. V rámci programu Digitální Evropa, ve vhodných případech doplněném výzkumnými a inovačními akcemi programu Horizont Evropa jako součást víceletého finančního rámce na období 2021–2027 navrhla Komise ambiciózní částku výlučně vyčleněnou na podporu testovacích center světové úrovně v Evropě.*

[18] COM(2018) 237.

[19] Budoucí Evropský obranný fond a stálá strukturovaná spolupráce (PESCO) rovněž poskytnou příležitosti pro výzkum a vývoj v oblasti umělé inteligence. Tyto projekty by měly být synchronizovány s rozsáhlejšími civilními programy EU zaměřenými na umělou inteligenci.

C. DOVEDNOSTI

Evropský přístup k umělé inteligenci bude muset být podpořen silným zaměřením na dovednosti, aby se vyřešil nedostatek kompetencí[20]. Komise brzy předloží rozšířenou agendu dovedností, jejímž cílem je zajistit, aby v Evropě mohl každý těžit z ekologické a digitální transformace ekonomiky EU. Iniciativy by rovněž mohly zahrnovat podporu pro odvětvové regulační orgány ke zlepšení jejich dovedností v oblasti umělé inteligence, aby mohly účinně a účelně provádět příslušná pravidla. Aktualizovaný akční plán digitálního vzdělávání pomůže lépe využívat data a technologie založené na umělé inteligenci, jako je analytika učení a prediktivní analýza, ke zlepšení systémů vzdělávání a odborné přípravy a jejich přizpůsobení digitálnímu věku. Plán rovněž zvýší povědomí o umělé inteligenci na všech úrovních vzdělávání s cílem připravit občany na informovaná rozhodnutí, která budou umělou inteligencí stále více ovlivněna.

Prioritou revidovaného koordinovaného plánu v oblasti umělé inteligence, který má být vypracován s členskými státy, bude rozvoj dovedností potřebných pro práci v oblasti umělé inteligence a prohlubování dovedností pracovníků, aby byli způsobilí pro transformaci založenou na umělé inteligenci. Mohlo by to zahrnovat přeměnu hodnotícího seznamu etických pokynů na orientační „osnovy“ pro vývojáře umělé inteligence, které budou zpřístupněny jako zdroj pro vzdělávací instituce. Je třeba vyvinout zvláštní úsilí, aby se zvýšil počet žen vyškolených a zaměstnaných v této oblasti.

Kromě toho by průkopnické centrum výzkumu a inovací v oblasti umělé inteligence v Evropě přilákalo díky možnostem, které by mohlo nabídnout, talenty z celého světa. Rovněž by došlo k rozvoji a šíření dovedností špičkové úrovně, které v celé Evropě vznikají a rozvíjejí se.

- *Opatření č. 3: Zřídit a podporovat pilíř pokročilých dovedností v rámci sítí předních vysokých škol a vysokoškolských institucí v programu Digitální Evropa s cílem přilákat nejlepší profesory a vědce a nabízet špičkové magisterské programy v oboru umělé inteligence.*

Kromě prohlubování dovedností se pracovníků a zaměstnanců přímo dotýká i vývoj a používání systémů umělé inteligence na pracovišti. Klíčovým faktorem při zajišťování přístupu k umělé inteligenci na pracovišti, který je zaměřen na člověka, bude zapojení sociálních partnerů.

D. ZAMĚŘENÍ NA MALÉ A STŘEDNÍ PODNIKY

Rovněž bude důležité zajistit, aby přístup k umělé inteligenci měly i malé a střední podniky a mohly ji využívat. Proto by měla být dále posílena centra pro digitální inovace[21] a platforma tzv. umělé inteligence na vyžádání[22] a měla by se rozšířit spolupráce mezi malými a středními podniky. K dosažení těchto cílů bude přispívat program Digitální Evropa. Zatímco by podporu malým a středním podnikům, aby pochopily přínosy umělé inteligence a přijaly ji, měla poskytovat všechna centra pro digitální inovace, bude důležité, aby alespoň jedno inovační centrum v každém členském státě bylo vysoce specializované na umělou inteligenci.

Aby mohly malé a střední podniky a startupy přizpůsobit své postupy nebo inovace za použití umělé inteligence, budou potřebovat přístup k financování. Komise v návaznosti na připravovaný pilotní investiční fond pro umělou inteligenci a technologii blockchain v hodnotě 100 milionů EUR plánuje

[20] https://ec.europa.eu/jrc/en/publication/academic-offer-and-demand-advanced-profiles-eu

[21] ec.europe.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities.

[22] www.Ai4eu.eu.

další rozšíření přístupu k financování umělé inteligence v rámci InvestEU[23]. Umělá inteligence je výslovně uvedena mezi způsobilými oblastmi pro využití záruky InvestEU.

- *Opatření č. 4: Komise bude spolupracovat s členskými státy s cílem zajistit, aby alespoň jedno centrum pro digitální inovace v každém členském státě bylo vysoce specializované na umělou inteligenci. Centra pro digitální inovace mohou být podporována v rámci programu Digitální Evropa.*
- *Komise a Evropský investiční fond zahájí v prvním čtvrtletí roku 2020 pilotní projekt ve výši 100 milionů EUR s cílem poskytnout kapitálové financování pro inovativní vývoj v oblasti umělé inteligence. S výhradou konečné dohody o víceletém finančním rámci je záměrem Komise výrazně tyto prostředky od roku 2021 navýšit prostřednictvím InvestEU.*

E. PARTNERSTVÍ SE SOUKROMÝM SEKTOREM

Je rovněž nezbytné zajistit, aby soukromý sektor byl plně zapojen do stanovování programu výzkumu a inovací a aby poskytoval potřebnou úroveň společných investic. To vyžaduje vytvoření široce pojatého partnerství veřejného a soukromého sektoru a odhodlanost nejvyššího vedení společností.

- *Opatření č. 5: V kontextu programu Horizont Evropa Komise zřídí nové partnerství veřejného a soukromého sektoru v oblasti umělé inteligence, dat a robotiky s cílem spojit úsilí, zajistit koordinaci výzkumu a inovací v této oblasti, spolupracovat s dalšími partnerstvími veřejného a soukromého sektoru v rámci programu Horizont Evropa a spolupracovat se zkušebními zařízeními a výše uvedenými centry pro digitální inovace.*

F. PODPORA ZAVÁDĚNÍ UMĚLÉ INTELIGENCE VE VEŘEJNÉM SEKTORU

Je zásadně důležité, aby orgány veřejné správy, nemocnice, veřejné služby a dopravní služby, orgány finančního dohledu a další oblasti veřejného zájmu urychleně začaly při svých činnostech používat produkty a služby, které využívají umělou inteligenci. Zvláštní důraz bude kladen na oblast zdravotní péče a dopravy, kde je technologie dostatečně rozvinutá pro rozsáhlé zavádění.

- *Opatření č. 6: Komise zahájí otevřené a transparentní odvětvové dialogy, v nichž upřednostní zdravotní péči, správy venkovských oblastí a provozovatele veřejných služeb s cílem předložit akční plán pro usnadnění rozvoje a zavádění umělé inteligence a experimentování v této oblasti. Odvětvové dialogy se využijí k přípravě specifického „Programu na zavádění umělé inteligence“, který podpoří zadávání veřejných zakázek na systémy umělé inteligence a pomůže přeměnit samotné postupy zadávání veřejných zakázek.*

G. ZAJIŠTĚNÍ PŘÍSTUPU K DATŮM A VÝPOČETNÍ INFRASTRUKTUŘE

Oblasti činnosti uvedené v této bílé knize doplňují plán, který je předkládán souběžně v rámci evropské strategie pro data. Zlepšení přístupu k datům a jejich správa jsou klíčové. Bez dat není vývoj umělé inteligence a dalších digitálních aplikací možný. Obrovský objem nových dat, která mají být teprve vytvořena, představuje pro Evropu příležitost, aby se dostala na přední pozici při transformaci v oblasti dat a umělé inteligence. Podpora odpovědných postupů pro správu dat a zajištění souladu dat se

[23]Europe.eu/investeu.

zásadami FAIR přispěje k budování důvěry a zajištění opětovné použitelnosti dat[24]. Stejně důležité jsou investice do klíčových počítačových technologií a infrastruktur.

Komise v rámci programu Digitální Evropa navrhla částku převyšující 4 miliardy EUR na podporu vysoce výkonné a kvantové výpočetní techniky, včetně edge computingu a umělé inteligence, dat a cloudové infrastruktury. Tyto priority dále rozvíjí Evropská strategie pro data.

H. MEZINÁRODNÍ HLEDISKA

Evropa má dobrou pozici pro to, aby hrála celosvětově vedoucí úlohu při vytváření spojenectví, pokud jde o společné hodnoty a podporu etického používání umělé inteligence. Práce EU v oblasti umělé inteligence se již v mezinárodních jednáních projevila. Při vypracovávání etických pokynů byla v odborné skupině na vysoké úrovni zapojena řada organizací mimo EU a několik vládních pozorovatelů. Současně se EU úzce zapojila do formulování etických zásad OECD pro umělou inteligenci[25]. Skupina G20 tyto zásady následně schválila ve svém prohlášení ministrů o obchodu a digitální ekonomice z června 2019.

EU současně uznává, že významné úsilí v oblasti umělé inteligence probíhá i na jiných mnohostranných fórech, včetně Rady Evropy, Organizace OSN pro výchovu, vědu a kulturu (UNESCO), Organizace pro hospodářskou spolupráci a rozvoj (OECD), Světové obchodní organizace a Mezinárodní telekomunikační unie (ITU). V OSN je EU zapojena do navazujících jednání týkajících se zprávy panelu na vysoké úrovni o digitální spolupráci, i do vypracování doporučení ohledně umělé inteligence.

EU bude v oblasti umělé inteligence i nadále spolupracovat se zeměmi s podobnými postoji, ale i s globálními aktéry a uplatňovat přístup založený na pravidlech a hodnotách EU (např. podpora většího sbližování právních předpisů, přístup k hlavním zdrojům včetně dat, vytvoření rovných podmínek). Komise bude pozorně sledovat politiky třetích zemí, které omezují tok dat, a bude řešit nepřiměřená omezení jak v rámci dvoustranných obchodních jednání, tak pomocí opatření v rámci Světové obchodní organizace. Komise je přesvědčena, že mezinárodní spolupráce v oblasti umělé inteligence musí vycházet z přístupu, který podporuje dodržování základních práv, včetně lidské důstojnosti, plurality, začlenění, nediskriminace a ochrany soukromí a osobních údajů[26], a bude usilovat o prosazování svých hodnot po celém světě[27]. Je rovněž zřejmé, že odpovědný rozvoj a používání umělé inteligence může být hnací silou pro dosažení cílů udržitelného rozvoje a dosažení pokroku v Agendě pro udržitelný rozvoj 2030.

[24] Dohledatelná, přístupná, interoperabilní a opakovaně použitelná (*Findable, Accessible, Interoperable and Reusable – FAIR*), jak je uvedeno v závěrečné zprávě a akčním plánu odborné skupiny Komise pro „FAIR“ data, 2018, https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

[25] https://www.oecd.org/going-digital/ai/principles/

[26] V rámci nástroje partnerství bude Komise financovat projekt v hodnotě 2,5 milionu EUR, který usnadní spolupráci s podobně smýšlejícími partnery s cílem podpořit etické pokyny EU v oblasti umělé inteligence a přijmout společné zásady a operační závěry.

[27] Předsedkyně Ursula von der Leyen, Unie, která si klade vyšší cíle – Moje agenda pro Evropu, s. 17.

5. EKOSYSTÉM DŮVĚRY: REGULAČNÍ RÁMEC PRO UMĚLOU INTELIGENCI

Používání jakékoli nové technologie s využitím umělé inteligence přináší jak příležitosti, tak i rizika. Občané se obávají, že s ohledem na informační asymetrie procesů rozhodování založených na algoritmech budou při obraně svých práv a bezpečnosti bezmocní, a podniky jsou znepokojeny právní nejistotou. Ačkoli umělá inteligence může pomoci chránit bezpečnost občanů a umožnit jim požívat svá základní práva, občané jsou zneklidněni tím, že umělá inteligence může mít nezamýšlené účinky nebo může být dokonce využívána k nekalým účelům. Tyto obavy je třeba řešit. Kromě toho, že chybí investice a dovednosti, je nedostatek důvěry hlavním faktorem, který širší využívání umělé inteligence brzdí.

Komise proto dne 25. dubna 2018 stanovila strategii pro umělou inteligenci[28], která se zaměřuje na socioekonomické aspekty a zároveň na zvýšení investic do výzkumu, inovací a kapacity pro umělou inteligenci v celé EU. Spolu s členskými státy schválila koordinovaný plán[29] s cílem sladit strategie. Komise rovněž zřídila odbornou skupinu na vysoké úrovni, která v dubnu 2019 vydala pokyny pro důvěryhodnou umělou inteligenci[30].

Komise zveřejnila sdělení[31], v němž vítá sedm klíčových požadavků stanovených v pokynech odborné skupiny na vysoké úrovni:

- Lidský faktor a dohled
- Technická spolehlivost a bezpečnost
- Ochrana soukromí a správa dat
- Transparentnost
- Rozmanitost, nediskriminace a spravedlnost
- Dobré sociální a environmentální podmínky
- Odpovědnost

Pokyny dále obsahují hodnotící seznam, který mají podniky používat v praxi. V průběhu druhé poloviny roku 2019 testovalo tento hodnotící seznam více než 350 organizací a zaslalo zpětnou vazbu. Odborná skupina na vysoké úrovni v současné době reviduje své pokyny s ohledem na tuto zpětnou vazbu, revize má být dokončena do června 2020. Jejím klíčovým výsledkem je zjištění, že i když se řada požadavků již odráží ve stávajících právních nebo regulačních režimech, nejsou v současné legislativě v mnoha hospodářských odvětvích pokryty požadavky týkající se transparentnosti, sledovatelnosti a lidského dohledu.

Kromě tohoto souboru nezávazných pokynů odborné skupiny na vysoké úrovni a v souladu s politickými směry předsedkyně by jasný evropský regulační rámec pomohl vytvořit důvěru mezi spotřebiteli a podniky v oblasti umělé inteligence, čímž by se zavádění této technologie urychlilo. Takový regulační rámec by měl jít ruku v ruce s dalšími opatřeními na podporu inovační kapacity Evropy a konkurenceschopnosti v této oblasti. Kromě toho musí zajistit optimální výsledky ze sociálního, environmentálního i hospodářského hlediska a soulad s právními předpisy, zásadami a hodnotami EU. To je obzvláště důležité v oblastech, kde mohou být práva občanů nejvíce dotčena, například v případě aplikací umělé inteligence pro prosazování práva a soudnictví.

[28] COM (2018) 237.
[29] COM (2018) 795.
[30] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top
[31] COM(2019) 168.

Na vývojáře i provozovatele umělé inteligence se již nyní vztahují evropské právní předpisy v oblasti základních práv (např. ochrana údajů, soukromí, zákaz diskriminace) a ochrany spotřebitele a pravidla týkající se bezpečnosti výrobků a odpovědnosti. Spotřebitelé očekávají stejnou úroveň bezpečnosti a dodržování svých práv bez ohledu na to, zda je výrobek nebo systém založen na umělé inteligenci, či nikoli. Uplatňování a prosazování těchto právních předpisů však mohou ztížit některé specifické rysy umělé inteligence (např. neprůhlednost). Z tohoto důvodu je třeba přezkoumat, zda jsou stávající právní předpisy schopny řešit rizika umělé inteligence a zda mohou být účinně prosazovány, zda jsou zapotřebí úpravy právních předpisů, nebo také nové právní předpisy.

Vzhledem k rychlému rozvoji umělé inteligence musí regulační rámec ponechat dostatečný prostor, aby se zohlednil i další vývoj. Veškeré změny by se měly omezovat na jasně určené problémy, pro něž existují proveditelná řešení.

Členské státy poukazují na současnou absenci společného evropského rámce. Německá komise pro etiku dat vyzvala k zavedení pětiúrovňového systému regulace na základě rizik, který by umožňoval nechat neškodné systémy umělé inteligence bez regulace, až po úplný zákaz pro ty nejnebezpečnější. Dánsko právě spustilo prototyp tzv. pečeti etiky dat. Malta zavedla dobrovolný systém certifikace pro umělou inteligenci. Pokud EU nestanoví přístup na úrovni EU, existuje reálné nebezpečí roztříštění vnitřního trhu, které by narušilo cíle, jimiž jsou důvěra, právní jistota a uvádění na trh.

Spolehlivý evropský regulační rámec pro důvěryhodnou umělou inteligenci ochrání všechny evropské občany a pomůže vytvořit hladce fungující vnitřní trh pro další rozvoj a zavádění umělé inteligence a také posílit evropský průmysl v oblasti umělé inteligence.

A. *VYMEZENÍ PROBLÉMU*

I když umělá inteligence může přinést mnoho pozitiv, například větší bezpečnost výrobků a postupů, může rovněž způsobit škody. Tato újma může být jak fyzická (bezpečnost a zdraví jednotlivců, včetně ztrát na životech, poškození majetku), tak nehmotná (ztráta soukromí, omezení práva na svobodu projevu, nerespektování lidské důstojnosti, diskriminace například v přístupu k zaměstnání atd.) a může souviset s celou řadou rizik. Regulační rámec by se měl soustředit na to, jak minimalizovat rizika různých možných škod, zejména těch nejvýznamnějších.

Hlavní rizika spojená s používáním umělé inteligence se týkají uplatňování pravidel, jejichž účelem je ochrana základních práv (včetně ochrany osobních údajů a soukromí a nediskriminace), jakož i otázek souvisejících s bezpečností[32] a odpovědností.

Rizika pro dodržování základních práv, včetně ochrany osobních údajů a soukromí a nediskriminace

Používání umělé inteligence může mít dopad na hodnoty, na nichž je EU založena, a vést k porušování základních práv[33], včetně svobody projevu, svobody shromažďování, práva na lidskou důstojnost, nediskriminace na základě pohlaví, rasového nebo etnického původu, náboženského vyznání nebo přesvědčení, zdravotního postižení, věku nebo sexuální orientace (podle konkrétních oblastí), ochrany

[32] Patří sem otázky kybernetické bezpečnosti, otázky spojené s aplikacemi umělé inteligence v kritických infrastrukturách nebo zneužití umělé inteligence pro nekalé účely.

[33] Z výzkumu Rady Evropy vyplývá, že využívání umělé inteligence by mohlo mít vliv na mnoho základních práv, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

osobních údajů a soukromí[34] nebo práva na účinnou soudní ochranu a spravedlivý proces, jakož i ochranu spotřebitele. Tato rizika mohou vyplývat z chybné koncepce systémů umělé inteligence (a to, i pokud jde o lidský dohled) nebo z použití dat bez korekce možného zkreslení (např. systém je trénován za použití pouze nebo hlavně údajů týkajících se mužů, což vede k neoptimálnímu výsledku ve vztahu k ženám).

Umělá inteligence může zastávat řadu funkcí, které dříve mohli vykonávat pouze lidé. V důsledku toho se budou občané a právní subjekty stále více setkávat s opatřeními a rozhodnutími přijatými systémy umělé inteligence nebo s jejich pomocí, která mohou být někdy obtížně srozumitelná a proti kterým může být v případě nutnosti obtížné se účinně bránit. Umělá inteligence navíc zvyšuje možnosti sledování a analýzy každodenních návyků lidí. Existuje například potenciální riziko, že umělou inteligenci mohou v rozporu s pravidly EU na ochranu údajů a jinými pravidly používat státní orgány nebo jiné subjekty k hromadnému sledování nebo zaměstnavatelé ke sledování chování svých zaměstnanců. Na základě analýzy velkého množství dat a identifikačních odkazů mezi nimi může být umělá inteligence rovněž využita ke zpětnému dohledání a deanonymizaci údajů o osobách, čímž vznikají nová rizika pro ochranu osobních údajů, a to i v případě datových souborů, které samy o sobě osobní údaje nezahrnují. Umělá inteligence je rovněž využívána online zprostředkovateli, kteří informace pro své uživatele třídí podle priorit a provádějí moderování obsahu. Zpracovávaná data, způsob navrhování aplikací a prostor pro zásah člověka mohou ovlivnit práva na svobodu projevu, ochranu osobních údajů, soukromí a politické svobody.

Některé algoritmy umělé inteligence, které se využívají k předpovídání recidivy trestné činnosti, mohou vykazovat genderovou a rasovou předpojatost a ukázat odlišnou pravděpodobnost recidivy u žen oproti mužům nebo u státních příslušníků daného státu ve srovnání s cizinci. *Zdroj: Tolan S., Miron M., Gomez E. and Castillo C. „Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia", Best Paper Award, International Conference on AI and Law, 2019*

Některé programy umělé inteligence pro analýzu obličeje vykazují genderovou a rasovou předpojatost, což ukazuje nízká chybovost při určování pohlaví mužů se světlejší pletí, ale vysokou chybovost při určování pohlaví u žen tmavší pleti. Zdroj: *Joy Buolamwini, Timnit Gebru; Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018.*

Předpojatost a diskriminace jsou přirozená rizika spojená s jakoukoli společenskou nebo hospodářskou činností. Rozhodování lidí není vůči chybám a předsudkům imunní. Tatáž tendence by však u umělé inteligence mohla mít mnohem větší dopady, bez mechanismů sociální kontroly, jimiž se řídí lidské chování, by mohla zasáhnout a diskriminovat mnoho lidí[35]. To může nastat i tehdy, když se systém umělé inteligence „učí" během provozu. V případech, kdy výsledek nemohl být ve fázi návrhu

[34] Těmito riziky se zabývá obecné nařízení o ochraně osobních údajů a směrnice o soukromí a elektronických komunikacích (nové nařízení o soukromí a elektronických komunikacích se projednává), ale možná bude třeba přezkoumat, zda systémy umělé inteligence nepřinášejí další rizika. Komise bude průběžně sledovat a posuzovat uplatňování obecného nařízení o ochraně osobních údajů.

[35] Poradní výbor Evropské komise pro rovné příležitosti žen a mužů v současné době připravuje „stanovisko k umělé inteligenci" obsahující mimo jiné analýzu dopadů umělé inteligence na rovnost žen a mužů, které má výbor přijmout na začátku roku 2020. Strategie EU pro rovnost žen a mužů na období 2020–2024 se rovněž zabývá spojitostí mezi umělou inteligencí a rovností žen a mužů. Evropská síť orgánů pro rovné zacházení (Equinet) zveřejní zprávu (vypracovanou společností Robin Allen a Debe Masters): „Regulace umělé inteligence: nová úloha orgánů pro rovné zacházení – nové problémy v oblasti rovnosti a nediskriminace vyplývající z větší digitalizace a využívání umělé inteligence", jejíž dokončení se očekává počátkem roku 2020.

předjímán nebo se mu nedalo předejít, nejsou příčinou rizik chyby v původním návrhu systému, ale spíše praktické dopady korelací nebo vzorců, které systém identifikuje v rozsáhlém souboru údajů.

Specifické vlastnosti mnoha technologií umělé inteligence, včetně neprůhlednosti („efekt černé skříňky“), složitosti, nepředvídatelnosti a částečného autonomního chování, mohou vést k tomu, že je obtížné ověřovat dodržování předpisů, a mohou bránit účinnému prosazování pravidel stávajícího práva Unie, jejichž cílem je ochrana základních práv. Donucovací orgány a dotčené osoby nemusí disponovat prostředky k ověření toho, jak bylo dané rozhodnutí se zapojením umělé inteligence učiněno, a tudíž zda byla dodržena příslušná pravidla. Fyzické a právnické osoby mohou mít obtíže s účinným přístupem ke spravedlnosti v situacích, kdy na ně tato rozhodnutí mohou mít negativní dopad.

Rizika pro bezpečnost a účinné fungování režimu odpovědnosti

Pokud jsou technologie umělé inteligence součástí výrobků a služeb, mohou pro uživatele představovat nová bezpečnostní rizika. Například v důsledku chyby v technologii rozpoznávání předmětů může autonomní automobil nesprávně identifikovat objekt na silnici a způsobit nehodu, při níž dojde ke zranění a materiálním škodám. Rizika pro základní práva mohou být způsobena nedostatky v návrhu technologie umělé inteligence, mohou souviset s problémy s dostupností a kvalitou dat nebo s jinými problémy vyplývajícími ze strojového učení. Zatímco některá z těchto rizik nejsou omezena na výrobky a služby, které jsou závislé na umělé inteligenci, používání umělé inteligence může toto riziko zvýšit nebo zhoršit.

Nedostatek jasných bezpečnostních opatření k řešení takových rizik může kromě rizik pro dotčené osoby vytvářet také právní nejistotu pro podniky, které uvádějí své výrobky využívající umělou inteligenci na trh v EU. Orgány dozoru nad trhem a donucovací orgány se mohou ocitnout v situaci, kdy není jasné, zda mohou zasáhnout, protože nemusí být zmocněny jednat a/nebo nemají vhodné technické možnosti pro kontrolu systémů[36]. Právní nejistota tedy může snížit celkovou úroveň bezpečnosti a podkopávat konkurenceschopnost evropských společností.

Pokud se bezpečnostní rizika naplní, je z důvodu nedostatku jasných požadavků a kvůli výše uvedeným vlastnostem technologií umělé inteligence obtížné zpětně vysledovat potenciálně problematická rozhodnutí učiněná za účasti systémů umělé inteligence. To může osobám, které utrpěly škodu, ztížit získání náhrady podle stávajících právních předpisů EU a vnitrostátních právních předpisů týkajících se odpovědnosti[37].

[36] Příkladem mohou být chytré hodinky pro děti. Tento výrobek nemusí dítěti přímo způsobit újmu, avšak bez zajištění minimální úrovně bezpečnosti, může být snadno použit jako nástroj pro přístup k dítěti. Orgány dozoru nad trhem mohou stěží zasáhnout v případech, kdy riziko není spojeno s výrobkem jako takovým.

[37] Jaké důsledky týkající se umělé inteligence, internetu věcí a dalších digitálních technologií je třeba vyvodit v právních předpisech v oblasti bezpečnosti a odpovědnosti, analyzuje zpráva Komise připojená k této bílé knize.

Podle směrnice o odpovědnosti za výrobky je výrobce odpovědný za škodu způsobenou vadným výrobkem. V případě systému založeného na umělé inteligenci, jako jsou autonomní automobily, však může být obtížné prokázat vadu výrobku, nastalou škodu a příčinnou souvislost mezi nimi. Kromě toho panuje určitá nejistota ohledně toho, jak a do jaké míry se směrnice o odpovědnosti za výrobky použije v případě určitých typů vad, například pokud vyplývají z nedostatků v kybernetické bezpečnosti výrobku.

Obtíže spojené se zpětným dohledáním potenciálně problematických rozhodnutí přijatých systémy umělé inteligence, které jsou zmíněny výše ve vztahu k základním právům, se tedy týkají rovněž otázek souvisejících s bezpečností a odpovědností. Může se stát, že osoby, které utrpěly škodu, nebudou mít účinný přístup k důkazům, které jsou nezbytné k tomu, aby případ mohl řešit soud, a mohou mít k dispozici méně účinné možnosti nápravy ve srovnání se situacemi, kdy je škoda způsobena tradičními technologiemi. Tato rizika se budou s větším využíváním umělé inteligence zvyšovat.

B. MOŽNÉ ÚPRAVY STÁVAJÍCÍHO PRÁVNÍHO RÁMCE EU V OBLASTI UMĚLÉ INTELIGENCE

Rozsáhlý soubor stávajících právních předpisů EU v oblasti bezpečnosti výrobků a odpovědnosti za ně[38], včetně odvětvových pravidel, který je dále doplněn vnitrostátními právními předpisy, je relevantní a potenciálně použitelný na řadu nových aplikací umělé inteligence.

Pokud jde o ochranu základních práv a práv spotřebitelů, legislativní rámec EU zahrnuje právní předpisy, jako je směrnice o rasové rovnosti[39], směrnice o rovném zacházení v zaměstnání a povolání[40], směrnice o rovném zacházení s muži a ženami, pokud jde o přístup k zaměstnání, a přístup ke zboží a službám[41], řada pravidel na ochranu spotřebitele[42], jakož i pravidla o ochraně osobních údajů a soukromí, zejména obecné nařízení o ochraně osobních údajů a další odvětvové právní předpisy týkající se ochrany osobních údajů, jako je směrnice o prosazování práva[43]. Kromě toho od roku 2025 začnou platit pravidla týkající se požadavků na přístupnost zboží a služeb stanovená v Evropském aktu přístupnosti[44]. Kromě toho musí být při provádění jiných právních předpisů EU, včetně oblasti finančních služeb, migrace nebo odpovědnosti online zprostředkovatelů, dodržována základní práva.

I když právní předpisy EU zůstávají v zásadě plně použitelné bez ohledu na zapojení umělé inteligence, je důležité posoudit, zda je možné je náležitě prosazovat při řešení rizik, která vytvářejí systémy umělé inteligence, nebo zda jsou zapotřebí úpravy konkrétních právních nástrojů.

Například hospodářské subjekty jsou i nadále plně odpovědné za to, aby umělá inteligence byla v souladu se stávajícími pravidly na ochranu spotřebitelů, jakékoli algoritmické využívání chování spotřebitelů je v rozporu se stávajícími pravidly a není povoleno a porušování práv musí být tudíž trestáno.

[38] Právní rámec EU pro bezpečnost výrobků sestává ze směrnice o obecné bezpečnosti výrobků (směrnice 2001/95/ES) jakožto záchranné sítě a řady odvětvových pravidel pokrývajících různé kategorie výrobků, od strojů, letadel a automobilů až po hračky a zdravotnické prostředky s cílem zajistit vysokou úroveň ochrany zdraví a bezpečnosti. Právní předpisy o odpovědnosti za výrobky jsou doplněny různými systémy občanskoprávní odpovědnosti za škody způsobené výrobky nebo službami.

[39] Směrnice 2000/43/ES.

[40] Směrnice 2000/78/ES.

[41] směrnice 2004/113/ES; Směrnice 2006/54/ES.

[42] Jako je směrnice o nekalých obchodních praktikách (směrnice 2005/29/ES) a směrnice o právech spotřebitelů (směrnice 2011/83/ES).

[43] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů.

[44] Směrnice (EU) 2019/882 o požadavcích na přístupnost u výrobků a služeb.

Komise se domnívá, že legislativní rámec by mohl být zdokonalen tak, aby řešil následující rizika a situace:

- *Účinné uplatňování a prosazování stávajících právních předpisů EU a vnitrostátních právních předpisů:* hlavní charakteristiky umělé inteligence představují problémy pro zajištění řádného uplatňování a prosazování právních předpisů EU a vnitrostátních právních předpisů. Kvůli nedostatečné transparentnosti (neprůhlednost umělé inteligence) je obtížné určit a prokázat případné porušení právních předpisů, včetně právních ustanovení na ochranu základních práv, určit odpovědnost a splnit podmínky pro uplatnění nároku na náhradu škody. V zájmu zajištění účinného uplatňování a prosazování předpisů proto může být nezbytné stávající právní předpisy v některých oblastech upravit nebo vyjasnit, například v oblasti odpovědnosti, jak je podrobněji uvedeno ve zprávě, která je přiložena k této bílé knize.

- *Omezení působnosti stávajících právních předpisů EU:* Právní předpisy EU v oblasti bezpečnosti výrobků se zaměřují zejména na uvádění výrobků na trh. Zatímco v právních předpisech EU týkajících se bezpečnosti výrobků musí software, pokud je součástí konečného produktu, splňovat příslušná bezpečnostní pravidla, nabízí se otázka, zda se na samostatný software vztahují právní předpisy EU o bezpečnosti výrobků, výjimkou jsou některá odvětví s pevně stanovenými pravidly[45]. V současnosti platné všeobecné právní předpisy EU v oblasti bezpečnosti se vztahují na výrobky, nikoli však na služby, a tedy v podstatě ani na služby založené na technologii umělé inteligence (např. zdravotnické služby, finanční služby, dopravní služby).

- *Měnící se rozsah funkcí systémů umělé inteligence:* Integrace softwaru, včetně umělé inteligence, do výrobků může změnit fungování těchto výrobků a systémů během jejich životního cyklu. To platí zejména pro systémy, které vyžadují časté aktualizace softwaru nebo které jsou založeny na strojovém učení. Tyto vlastnosti mohou vést ke vzniku nových rizik, která nebyla při uvedení systému na trh přítomna. Uvedená rizika nejsou ve stávajících právních předpisech, které se zaměřují především na bezpečnostní rizika přítomná v době uvedení na trh, dostatečně řešena.

- *Nejistota ohledně rozdělení odpovědnosti mezi jednotlivé hospodářské subjekty v dodavatelském řetězci:* Právní předpisy EU týkající se bezpečnosti výrobků obecně přiřazují odpovědnost výrobci výrobku uvedeného na trh, a to včetně všech jeho složek, např. systémů umělé inteligence. Pokud je však například umělá inteligence doplněna po uvedení výrobku na trh další stranou, která není výrobcem, mohou vzniknout nejasnosti v pravidlech. Právní předpisy EU týkající se odpovědnosti za vadné výrobky navíc stanoví odpovědnost výrobců a vnitrostátní pravidla odpovědnosti pak upravují odpovědnost ostatních subjektů v dodavatelském řetězci.

- *Změny koncepce bezpečnosti:* používání umělé inteligence v produktech a službách může vést k rizikům, jimiž se právní předpisy EU v současné době výslovně nezabývají. Tato rizika mohou být spojena s kybernetickými hrozbami, osobními bezpečnostními riziky (například v souvislosti s novými aplikacemi umělé inteligence, např. pro domácí spotřebiče), riziky, která

[45] Například software určený výrobcem pro lékařské účely je považován za zdravotnický prostředek podle nařízení o zdravotnických prostředcích (nařízení (EU) 2017/745).

jsou důsledkem ztráty konektivity atd. Tato rizika mohou být přítomna při uvádění výrobků na trh nebo mohou vzniknout v důsledku aktualizací softwaru nebo být výsledkem samostatného učení při používání produktu. EU by měla plně využívat nástrojů, které má k dispozici, k posílení své důkazní základny o potenciálních rizicích spojených s aplikacemi umělé inteligence, a to i s využitím zkušeností Agentury Evropské unie pro kybernetickou bezpečnost (ENISA), aby mohly být posouzeny formy hrozeb vyplývajících z umělé inteligence.

Jak je uvedeno výše, několik členských států již zkoumá možnosti vnitrostátních právních předpisů pro řešení problémů způsobených umělou inteligencí. To zvyšuje riziko, že dojde k roztříštění jednotného trhu. Různorodé vnitrostátní předpisy pravděpodobně povedou k vytvoření překážek pro společnosti, které chtějí prodávat a provozovat systémy umělé inteligence na jednotném trhu. Zajištění společného přístupu na úrovni EU by evropským společnostem umožnilo těžit z bezproblémového

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

Zpráva, která je přiložena k této bílé knize, analyzuje příslušný právní rámec. Poukazuje na nejistoty, pokud jde o uplatňování tohoto rámce s ohledem na specifická rizika, která systémy umělé inteligence a jiné digitální technologie představují.

Dochází k závěru, že stávající právní předpisy v oblasti bezpečnosti výrobků již podporují rozšířenou koncepci bezpečnosti, která chrání před všemi druhy rizik plynoucích z produktu podle jeho použití. Pro zvýšení právní jistoty by však mohla být zavedena ustanovení, která by se výslovně vztahovala na nová rizika, které představují vznikající digitální technologie.

- Autonomní chování některých systémů umělé inteligence během jejich životního cyklu může mít za následek významné změny výrobku, které mají dopad na bezpečnost, což může vyžadovat nové posouzení rizik. Kromě toho může být potřebný lidský dohled nad návrhem výrobku a v průběhu celého životního cyklu výrobků a systémů umělé inteligence jako záruka.
- Rovněž by mohlo být zváženo zavedení výslovných povinností pro výrobce, a to případně také s ohledem na rizika pro psychické zdraví uživatelů (např. spolupráce s humanoidními roboty).
- Právní předpisy Unie v oblasti bezpečnosti výrobků by mohly stanovit zvláštní požadavky týkající se bezpečnostních rizik souvisejících s chybnými údaji ve fázi návrhu a také mechanismů pro zajištění toho, aby byla kvalita údajů zachována po celou dobu používání výrobků a systémů umělé inteligence.
- Neprůhlednost systémů založených na algoritmech by mohla být řešena zavedením požadavků na transparentnost.
- V případě samostatného softwaru uváděného takto na trh nebo softwaru staženého do výrobku po jeho uvedení na trh, který má dopad na bezpečnost, může být nutné stávající pravidla upravit a vyjasnit.
- Vzhledem ke stále větší složitosti dodavatelských řetězců, pokud jde o nové technologie, by mohla právní jistotu poskytnout ustanovení, která by konkrétně vyžadovala spolupráci mezi hospodářskými subjekty v dodavatelském řetězci a uživateli.

Vlastnosti vznikajících digitálních technologií, jako je umělá inteligence, internet věcí a robotika, mohou zpochybnit určité aspekty rámce odpovědnosti a mohly by snížit jeho účinnost. Některé z těchto vlastností by mohly ztížit zpětné dohledání osoby, která škodu způsobila, což je podle většiny vnitrostátních pravidel nezbytné pro uplatnění nároku na odškodnění na základě zavinění. Mohly by se tak výrazně zvýšit náklady pro oběti a uplatnění nebo prokázání nároků vůči jiným osobám než výrobcům by mohlo být obtížné.

- Osoby, které utrpěly škodu v důsledku zapojení systémů umělé inteligence, musí požívat stejné úrovně ochrany jako osoby, které utrpěly újmu způsobenou jinými technologiemi, přičemž je třeba umožnit, aby se technologické inovace i nadále vyvíjely.
- Všechny možnosti k zajištění tohoto cíle by měly být pečlivě posouzeny, včetně možných změn směrnice o odpovědnosti za výrobky a případné další cílené harmonizace vnitrostátních pravidel týkajících se odpovědnosti. Komise se například snaží zjistit, zda a do jaké míry může být potřeba zmírnit následky složitosti přizpůsobením důkazního břemene vyžadovaného vnitrostátními pravidly o odpovědnosti za škodu způsobenou provozem aplikací umělé inteligence.

přístupu na jednotný trh a podpořit jejich konkurenceschopnost na celosvětových trzích.

Na základě výše uvedeného Komise dochází k závěru, že kromě možných úprav stávajících právních předpisů mohou být zapotřebí nové právní předpisy zaměřené specificky na umělou inteligenci, aby se právní rámec EU přizpůsobil současnému a očekávanému vývoji technologií a obchodu.

C. OBLAST PŮSOBNOSTI BUDOUCÍHO REGULAČNÍHO RÁMCE EU

Klíčovou otázkou budoucího zvláštního regulačního rámce pro umělou inteligenci je určit rozsah jeho uplatňování. Prozatím se vychází se z předpokladu, že regulační rámec by se vztahoval na výrobky a služby využívající umělou inteligenci. Pro účely této bílé knihy by proto měla být umělá inteligence jasně definována, stejně jako jakákoli případná budoucí iniciativa v oblasti tvorby politik.

Komise ve svém sdělení o umělé inteligenci pro Evropu předložila první definici umělé inteligence[46]. Tuto definici dále upřesnila odborná skupina na vysoké úrovni[47].

Ve veškerých nových právních nástrojích bude třeba, aby definice umělé inteligence byla dostatečně flexibilní, aby se přizpůsobila technickému pokroku, a zároveň byla dostatečně přesná, aby poskytla potřebnou právní jistotu.

Pro účely této bílé knihy i všech případných budoucích diskusí o politických iniciativách se zdá být důležité vyjasnit hlavní prvky, které tvoří umělou inteligenci, tj. „data“ a „algoritmy“. Umělá inteligence může být integrována v hardwaru. V případě technik strojového učení, které tvoří podmnožinu umělé inteligence, jsou algoritmy trénovány tak, aby odvozovaly určité vzorce založené na souboru dat, podle nichž určí činnosti potřebné k dosažení daného cíle. Algoritmy se mohou při používání dále učit. I když výrobky založené na umělé inteligenci mohou jednat samostatně tím, že vnímají prostředí, v němž fungují, a bez dodržení předem stanoveného souboru pokynů, jejich chování je z velké části vymezeno a omezeno jeho tvůrci. Lidé určují a programují cíle, pro jejichž plnění by měl být systém umělé inteligence optimalizován.

> Při autonomním řízení vozidel například algoritmus používá v reálném čase data z vozidla (rychlost, spotřeba motoru, tlumiče pérování atd.) a ze snímačů, které sledují celé okolní prostředí vozidla (silnice, značky, jiná vozidla, chodci atd.), k odvození směru, zrychlení a rychlosti, kterých by automobil měl dosáhnout, aby dojel do místa určení. Pomocí získaných dat se algoritmus přizpůsobuje situaci na silnici a vnějším podmínkám, včetně chování ostatních řidičů, aby odvodil parametry pro nejpohodlnější a nejbezpečnější jízdu.

EU má přísný právní rámec, který má mimo jiné zajistit ochranu spotřebitele, řešit nekalé obchodní praktiky a chránit osobní údaje a soukromí. Kromě toho obsahuje *acquis* pro některá odvětví

[46] COM(2018) 237 final, s. 1: „Za umělou inteligenci se považují systémy vykazující inteligentní chování v podobě vyhodnocování svého okolí a následného rozhodování či vykonávání kroků – s určitou mírou autonomie – k dosažení konkrétních cílů.
Systémy využívající technologii umělé inteligence mohou být čistě softwarové, které působí jen ve virtuálním světě (např. hlasoví asistenti, program na analýzu snímků, vyhledávače, systémy rozpoznávání hlasu a obličeje), nebo mohou být zabudovány do technického vybavení (např. pokročilé roboty, autonomní vozidla, drony a různé formy využití internetu věcí).“

[47] Odborná skupina na vysoké úrovni, definice umělé inteligence, s. 8: „Systémy umělé inteligence jsou softwarové (a případně také hardwarové) systémy navržené lidmi, které mají zadán složitý cíl a jednají ve fyzické nebo digitální dimenzi, přičemž vnímají své prostředí tím, že získávají data, interpretují shromážděná strukturovaná nebo nestrukturovaná data, usuzují ze znalostí nebo zpracovávají informace odvozené z těchto dat a rozhodují o nejlepší akci či akcích k dosažení daného cíle. Systémy umělé inteligence mohou používat symbolická pravidla nebo si vytvořit numerický model; mohou rovněž přizpůsobovat své chování na základě analýzy toho, jak je prostředí ovlivněno jejich předchozími akcemi.“

(např. zdravotnictví, dopravu) zvláštní pravidla. Tato stávající ustanovení práva Unie se budou v souvislosti s umělou inteligencí uplatňovat i nadále, mohou avšak být nezbytné určité aktualizace tohoto rámce, aby byla zohledněna digitální transformace a používání umělé inteligence (viz oddíl B). V důsledku toho se aspekty, jimiž se již zabývají stávající horizontální nebo odvětvové právní předpisy (např. o zdravotnických prostředcích[48], dopravních systémech), budou i nadále řídit těmito právními předpisy.

V podstatě by měl být nový regulační rámec pro umělou inteligenci účinný, aby dosáhl svých cílů, aniž by byl příliš normativní, že by vytvářel nepřiměřenou administrativní zátěž, zejména pro malé a střední podniky. V zájmu dosažení této rovnováhy se Komise domnívá, že je nutné řídit se přístupem založeným na posouzení rizik.

Přístup založený na posouzení rizik je důležitý pro zajištění toho, aby regulační intervence byla přiměřená. Vyžaduje však jasná kritéria pro rozlišování mezi různými aplikacemi umělé inteligence, zejména pokud jde o otázku, zda jsou, či nejsou „vysoce rizikové“[49]. Vymezení toho, co je vysoce riziková umělá inteligence, by mělo být jasné a snadno srozumitelné a použitelné pro všechny dotčené strany. Nicméně, i v případě, že aplikace umělé inteligence není kvalifikována jako vysoce riziková, zůstává zcela předmětem již existujících pravidel EU.

Komise zastává názor, že daná aplikace umělé inteligence by měla být obecně považována za vysoce rizikovou s ohledem na to, co je v sázce, a podle toho, zda je toto odvětví a zamýšlené použití spojeno s významnými riziky, zejména z hlediska ochrany bezpečnosti, práv spotřebitelů a základních práv. Konkrétně by použití umělé inteligence mělo být považováno za vysoce rizikové, pokud splňuje tato dvě kumulativní kritéria:

- Zaprvé, aplikace umělé inteligence se používá v odvětví, kde lze s ohledem na charakteristické rysy činností typicky očekávat významná rizika. Toto první kritérium zajišťuje, aby se regulační zásah zaměřil na oblasti, v nichž se obecně má za to, že se s největší pravděpodobností objeví rizika. Nový regulační rámec by měl stanovit úplný seznam konkrétních odvětví, která jsou zahrnuta. Například by sem měla patřit zdravotní péče, doprava, energetika a části veřejného sektoru[50]. Seznam by měl být pravidelně přezkoumáván a v případě potřeby pozměněn v závislosti na příslušném vývoji v praxi.
- Zadruhé, umělá inteligence v dotčeném odvětví se navíc používá takovým způsobem, že pravděpodobně hrozí značná rizika. Toto druhé kritérium odráží skutečnost, že ne každé použití umělé inteligence ve vybraných odvětvích nutně zahrnuje významná rizika. Například, i když zdravotní péče může být obecně relevantním odvětvím, chyba v systému pro plánování využití míst v nemocnici obvykle nepředstavuje riziko takového významu, který by odůvodňoval legislativní zásah. Úroveň rizika daného použití by mohla být posuzována podle dopadu na dotčené strany. Například použití aplikací umělé inteligence, které mají právní nebo podobně významné účinky na práva jednotlivce nebo společnosti; které představují riziko zranění, smrti nebo významné materiální či nehmotné újmy nebo které mají účinky, jimž se jednotlivci nebo právnické osoby nemohou přiměřeně vyhnout.

[48] Například u systémů umělé inteligence, které lékařům poskytují specializované lékařské informace, systémů umělé inteligence poskytujících lékařské informace přímo pacientům a systémů umělé inteligence, které provádějí lékařské úkony přímo na pacientovi, vyvstávají různé bezpečnostní otázky a vznikají právní důsledky. Komise zkoumá tyto problémy související s bezpečností a odpovědností, které jsou pro oblast zdravotní péče specifické.

[49] Právní předpisy EU mohou kategorizovat „rizika“ odlišně od toho, jak jsou popsána zde, v závislosti na oblasti, jako je například bezpečnost výrobků.

[50] Z veřejného sektoru by se mohlo jednat o oblasti, jako je azyl, migrace, hraniční kontroly a soudnictví, sociální zabezpečení a služby zaměstnanosti.

Použití dvou kumulativních kritérií by zajistilo správné stanovení rozsahu regulačního rámce a právní jistotu. Povinné požadavky obsažené v novém regulačním rámci pro umělou inteligenci (viz oddíl D níže) by se v zásadě vztahovaly pouze na ty aplikace, které byly označeny za vysoce rizikové v souladu s těmito dvěma kumulativními kritérii.

Bez ohledu na výše uvedené mohou rovněž nastat výjimečné případy, kdy je využití umělé inteligence vzhledem k rizikům, o která se jedná, pro určité účely považováno za vysoce rizikové, tj. bez ohledu na dotčené odvětví, a v tomto případě by se nadále uplatňovaly níže uvedené požadavky.[51] Pro ilustraci lze uvést tyto dva příklady:

- S ohledem na význam pro jednotlivce a vzhledem k *acquis* EU, jehož součástí je otázka rovnosti v oblasti zaměstnanosti, by používání aplikací umělé inteligence pro postupy přijímání zaměstnanců a v situacích, které mají dopad na práva pracovníků, mělo být vždy považováno za „vysoce rizikové“, a proto by se měly v každém případě uplatňovat níže uvedené požadavky. Bylo by možné zvážit další konkrétní aplikace, které mají dopad na práva spotřebitelů.

- Používání aplikací umělé inteligence pro účely biometrické identifikace na dálku[52] a jiných technologií narušujících soukromí, by vždy bylo považováno za „vysoce rizikové“, a proto by se vždy uplatňovaly níže uvedené požadavky.

D. DRUHY POŽADAVKŮ

Při navrhování budoucího regulačního rámce pro umělou inteligenci bude nutné rozhodnout o typech povinných zákonných požadavků, které mají být příslušným subjektům uloženy. Tyto požadavky mohou být dále upřesněny prostřednictvím norem. Jak je uvedeno v oddíle C výše, kromě již existujících právních předpisů by se tyto požadavky vztahovaly pouze na vysoce rizikové aplikace umělé inteligence, čímž by se zajistilo, že jakýkoli regulační zásah bude cílený a přiměřený.

S ohledem na pokyny odborné skupiny na vysoké úrovni a na skutečnosti uvedené výše by požadavky na vysoce rizikové aplikace umělé inteligence mohly sestávat z následujících klíčových prvků, které jsou podrobněji popsány v následujících pododdílech:

- tréninková data,
- data a vedení záznamů,
- informace, které mají být poskytovány,
- spolehlivost a přesnost,
- lidský dohled,
- zvláštní požadavky na určité aplikace umělé inteligence, jako např. požadavky používané pro účely biometrické identifikace na dálku.

V zájmu zajištění právní jistoty budou tyto požadavky dále upřesněny tak, aby poskytovaly jednoznačné reference pro všechny subjekty, které je musí splňovat.

a) Tréninková data

[51] Je důležité zdůraznit, že mohou platit i jiné právní předpisy EU. Například, pokud jsou aplikace umělé inteligence integrovány ve spotřebním výrobku, může se na bezpečnost aplikací umělé inteligence vztahovat směrnice o obecné bezpečnosti výrobků.

[52] Biometrická identifikace na dálku by se měla odlišovat od biometrického ověřování (což je bezpečnostní proces, který se opírá o jedinečné biologické vlastnosti jednotlivce k ověření jeho identity). Biometrické identifikace na dálku je určování totožnosti více osob pomocí biometrických identifikátorů (otisků prstů, zobrazení obličeje, duhovky, struktury žil atd.) na dálku ve veřejném prostoru nepřetržitě nebo průběžně, a to kontrolou oproti datům uloženým v databázi.

Prosazovat, posilovat a bránit hodnoty a pravidla EU, a zejména práva, která občané odvozují z práva Unie, je nyní důležitější než kdy jindy. Toto úsilí se bezpochyby vztahuje i na vysoce rizikové aplikace umělé inteligence, které jsou uváděny na trh a používány v EU.

Jak bylo uvedeno výše, umělá inteligence nemůže existovat bez dat. Fungování mnoha systémů a činností umělé inteligence a rozhodnutí, k nimž mohou vést, velmi závisí na souboru dat, na jejichž základě byly tyto systémy trénovány. Proto by měla být přijata nezbytná opatření k zajištění toho, aby v případě dat používaných pro trénování systémů umělé inteligence byly dodržovány hodnoty a pravidla EU, zejména pokud jde o bezpečnost a stávající právní předpisy na ochranu základních práv. Pro soubory dat používané pro trénování systémů umělé inteligence je možné zvážit tyto požadavky:

- Požadavky, jejichž cílem je poskytnout přiměřenou jistotu, že následné použití výrobků nebo služeb, které systém umělé inteligence umožňuje, je bezpečné, neboť splňuje standardy stanovené v platných bezpečnostních pravidlech EU (stávajících i případných doplňkových). Například požadavky na zajištění toho, aby byly systémy umělé inteligence trénovány na souborech dat, které jsou dostatečně široké a zahrnují všechny relevantní scénáře potřebné k tomu, aby se zabránilo nebezpečným situacím.

- Požadavky na přijetí přiměřených opatření, jejichž cílem je zajistit, aby takové následné používání systémů umělé inteligence nevedlo k výsledkům, které by měly za následek diskriminaci. Tyto požadavky by mohly zahrnovat zejména povinnosti používat soubory dat, které jsou dostatečně reprezentativní, zejména s cílem zajistit, aby byly všechny příslušné aspekty, jako pohlaví, etnický původ a další možné důvody nepřípustné diskriminace v těchto souborech dat náležitě zohledněny.

- Požadavky zaměřené na zajištění odpovídající ochrany soukromí a osobních údajů při používání produktů a služeb založených na umělé inteligenci. Příslušné záležitosti upravuje obecné nařízení o ochraně údajů a směrnice o prosazování práva, podle jejich oblasti působnosti.

b) Uchovávání záznamů a dat

S přihlédnutím k prvkům, jako je složitost a neprůhlednost mnoha systémů umělé inteligence, a s tím související obtíže, které mohou ztěžovat účinné ověřování dodržování a prosazování platných pravidel, jsou vyžadovány požadavky ohledně vedení záznamů o programování algoritmu, dat používaných pro trénování vysoce rizikových systémů umělé inteligence a v některých případech i uchovávání samotných dat. Tyto požadavky v zásadě umožňují zpětné vysledování a ověřování potenciálně problematických kroků nebo rozhodnutí systémů umělé inteligence, což by mělo nejen usnadnit dohled a prosazování práva, ale mohlo by se rovněž zvýšit pobídky pro dotčené hospodářské subjekty, aby ihned v počáteční fázi vzaly v potaz, že je nutné tato pravidla dodržovat.

Za tímto účelem by regulační rámec mohl stanovit, že by měly být uchovávány:

- přesné záznamy o souboru dat použitých k trénování a testování systémů umělé inteligence, včetně popisu hlavních charakteristik a způsobu výběru datového souboru,

- v některých odůvodněných případech samotné soubory dat,

- dokumentace o metodách programování[53] a trénování, postupech a technikách používaných při vytváření, testování a validaci systémů umělé inteligence, v příslušných případech i z hlediska bezpečnosti a předcházení zkreslení, které by mohlo vést k zakázané diskriminaci.

Záznamy, dokumentace a v příslušných případech datové soubory by měly být uchovávány po omezenou, přiměřenou dobu, aby bylo zajištěno účinné prosazování příslušných právních předpisů. Měla by být přijata opatření, která zajistí, že budou na požádání k dispozici, zejména při testování nebo inspekci ze strany příslušných orgánů. V případě potřeby by měla být přijata opatření k zajištění ochrany důvěrných informací, jako je obchodní tajemství.

c) Poskytování informací

Transparentnost je nutná i nad rámec požadavků na vedení záznamů uvedených v písmenu c) výše. Aby bylo dosaženo sledovaných cílů – zejména podpory odpovědného využívání umělé inteligence, budování důvěry a v případě potřeby usnadnění nápravy – je důležité, aby byly proaktivně poskytovány náležité informace o využívání vysoce rizikových systémů umělé inteligence.

V souladu s tím by bylo možné zvážit následující požadavky:

- Zajištění jasných informací, které je třeba poskytnout ohledně schopností a omezení systému umělé inteligence, zejména účel, pro který jsou tyto systémy určeny, podmínky, za nichž lze očekávat, že budou fungovat tak, jak je zamýšleno, a očekávanou míru přesnosti při dosahování stanoveného účelu. Tyto informace jsou důležité zejména pro provozovatele systémů, ale mohou být rovněž relevantní pro příslušné orgány a dotčené strany.

- Jednotlivě by měli být jasně informováni občané o tom, že komunikují se systémem umělé inteligence, a nikoli s lidskou bytostí. Ačkoli právní předpisy EU o ochraně údajů již obsahují určitá pravidla tohoto druhu[54], k dosažení výše uvedených cílů mohou být vyžadovány dodatečné požadavky. V případě, že tomu tak bude, je třeba se vyhnout zbytečné zátěži. Proto takové informace není třeba poskytovat například v situacích, kdy je občanům okamžitě zřejmé, že jsou v interakci se systémy umělé inteligence. Dále je důležité, aby poskytované informace byly objektivní, stručné a snadno srozumitelné. Způsob poskytování informací by měl být přizpůsoben konkrétní situaci.

d) Spolehlivost a přesnost

Systémy a vysoce rizikové aplikace umělé inteligence musí být nepochybně technicky spolehlivé a přesné, aby byly důvěryhodné. To znamená, že tyto systémy musí být vyvíjeny odpovědným způsobem a s náležitým předchozím zvážením rizik, která mohou vytvářet. Musí být vyvinuty a fungovat tak, aby bylo zajištěno, že systémy umělé inteligence se budou chovat spolehlivě, jak bylo zamýšleno. Měla by být přijata veškerá přiměřená opatření k minimalizaci rizika vzniku škody.

V souladu s tím by bylo možné zvážit následující prvky:

- požadavky na zajištění toho, aby systémy umělé inteligence byly spolehlivé a přesné nebo alespoň správně odrážely míru přesnosti během všech fází životního cyklu,

[53] Například dokumentace o algoritmu, včetně toho, co model optimalizací sleduje, jaká váha je pro určité parametry navržena v počáteční fázi atd.
[54] Zejména podle čl. 13 odst. 2 písm. f) obecného nařízení o ochraně osobních údajů musí správci v okamžiku získání osobních údajů poskytnout subjektům údajů další informace nezbytné pro zajištění spravedlivého a transparentního zpracování údajů o tom, že dochází k automatizovanému rozhodování, a některé další informace.

- požadavky zajišťující reprodukovatelnost výsledků,

- požadavky zajišťující, aby systémy umělé inteligence mohly odpovídajícím způsobem řešit chyby nebo nesrovnalosti během všech fází životního cyklu,

- požadavky, které zajistí, aby byly systémy umělé inteligence odolné jak proti zjevným útokům, tak vůči subtilnějším pokusům, aby data nebo algoritmy samy manipulovaly, a aby byla v takových případech přijata zmírňující opatření.

e) Lidský dohled

Dohled ze strany člověka pomáhá zajistit, aby systém umělé inteligence nepodkopával lidskou autonomii nebo neměl jiné negativní účinky. Cíle důvěryhodné, etické umělé inteligence zaměřené na člověka lze v souvislosti s vysoce rizikovými aplikacemi umělé inteligence dosáhnout pouze zajištěním vhodného zapojení lidí.

Ačkoli jsou všechny aplikace umělé inteligence, pro něž tato bílá kniha navrhuje zvláštní právní režim, považovány za vysoce rizikové, může se vhodný typ a míra lidského dohledu v jednotlivých případech lišit. Závisí zejména na zamýšleném použití systémů a na účincích, které by používání mohlo mít pro dotčené občany a právnické osoby. Pokud systém umělé inteligence zpracovává osobní údaje, neměla by být dotčena ani zákonná práva stanovená v obecném nařízení o ochraně osobních údajů. Lidský dohled by například mohl zahrnovat mimo jiné tyto prvky:

- výstup systému umělé inteligence nenabude účinnosti, pokud nebyl již dříve přezkoumán a ověřen člověkem (např. o zamítnutí žádosti o dávky sociálního zabezpečení může rozhodnout pouze člověk),

- výstup systému umělé inteligence má okamžitou účinnost, avšak následně je zajištěn zásah člověka (např. odmítnutí žádosti o kreditní kartu může být zpracováno systémem umělé inteligence, ale následně musí být možné, aby došlo k přezkumu rozhodnutí člověkem),

- sledování systému umělé inteligence v průběhu provozu a schopnost zasahovat v reálném čase a deaktivovat jej (např. v automobilech bez řidiče je k dispozici tlačítko nebo postup pro zastavení pro případy, kdy člověk určí, že provoz vozidla není bezpečný),

- ve vývojové fázi: možnost uložení provozních omezení systému umělé inteligence (např. automobil bez řidiče musí za určitých podmínek, jako je nízká viditelnost nebo pokud přestanou spolehlivě fungovat snímače, zastavit, nebo musí za daných podmínek udržovat určitou vzdálenost od předchozího vozidla).

f) Zvláštní požadavky na biometrickou identifikaci na dálku

Shromažďování a využívání biometrických údajů[55] pro identifikaci na dálku[56], například zavedením rozpoznávání obličeje ve veřejném prostoru, s sebou nese specifická rizika v oblasti základních práv[57].

[55] Biometrické údaje jsou vymezeny jako „osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje její jedinečnou autentizaci nebo identifikaci, například zobrazení obličeje nebo daktyloskopické (otisky prstů) údaje.“ (Ustanovení čl. 3 odst. 13 směrnice o prosazování práva, čl. 4 odst. 14 obecného nařízení o ochraně osobních údajů a čl. 3 odst. 18 nařízení (EU) 2018/1725).

Důsledky používání systémů umělé inteligence při biometrické identifikaci na dálku pro základní práva se mohou značně lišit v závislosti na účelu, kontextu a rozsahu používání.

Pravidla EU pro ochranu údajů v zásadě zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby s výjimkou výjimečných okolností[58] zakazují. Konkrétně z obecného nařízení o ochraně osobních údajů vyplývá, že k takovému zpracování může dojít pouze na základě omezeného počtu důvodů, přičemž hlavní důvod je významný veřejný zájem. V takovém případě musí zpracování probíhat na základě práva EU nebo vnitrostátního práva, s výhradou požadavků přiměřenosti, dodržování podstaty práva na ochranu údajů a vhodných záruk. Podle směrnice o prosazování práva musí být takové zpracování nezbytně nutné, v zásadě je potřeba povolení na základě práva Unie nebo vnitrostátních právních předpisů, jakož i vhodné záruky. Jakékoli zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby by se týkalo výjimky ze zákazu stanoveného v právu Unie a podléhalo by Listině základních práv Evropské unie.

Z toho vyplývá, že v souladu se stávajícími pravidly EU pro ochranu údajů a Listinou základních práv lze umělou inteligenci používat pro účely biometrické identifikace na dálku, pouze pokud je takové použití řádně odůvodněné, přiměřené a podléhá přiměřeným zárukám.

S cílem řešit případné společenské obavy týkající se využívání umělé inteligence pro tyto účely na veřejných místech a zabránit roztříštění vnitřního trhu zahájí Komise rozsáhlou evropskou diskusi o konkrétních případných okolnostech, které by mohly toto použití odůvodnit, a o společných zárukách.

E. URČENÍ

Pokud jde o to, komu jsou právní požadavky, které by se vztahovaly na výše uvedené vysoce rizikové aplikace umělé inteligence, určeny, je třeba vzít v úvahu dva hlavní aspekty.

Zaprvé vyvstává otázka rozdělení povinností mezi dotčené hospodářské subjekty. Do životního cyklu systému umělé inteligence je zapojeno mnoho aktérů. Patří mezi ně vývojář, provozovatel (osoba, která používá výrobek nebo službu, které jsou vybaveny systémem umělé inteligence) a případně další (výrobce, distributor nebo dovozce, poskytovatel služeb, profesionální nebo soukromý uživatel).

Komise je toho názoru, že v budoucím regulačním rámci by každá z těchto povinností měla být určena subjektu nebo subjektům, které jsou nejlépe schopny čelit jakýmkoli potenciálním rizikům. Například zatímco vývojáři umělé inteligence mohou být nejvhodnější úrovní pro řešení rizik vyplývajících z vývojové fáze, jejich schopnost kontrolovat rizika ve fázi používání může být omezenější. V takovém případě by se příslušné povinnosti měly vztahovat na provozovatele. Tím není dotčena otázka, která strana by pro účely odpovědnosti a zajištění účinného přístupu ke spravedlnosti, měla být odpovědná strana za jakoukoli škodu způsobenou konečnému uživateli nebo jiným stranám, které utrpěly újmu.

---

[56] V souvislosti s rozpoznáváním obličeje identifikace znamená, že šablona zobrazení obličeje dané osoby je srovnávána s mnoha jinými šablonami uloženými v databázi s cílem zjistit, zda je v databázi uchováváno její zobrazení. Autentizace (nebo ověřování) se na druhé straně často označuje jako párování (porovnání dvou šablon). Umožňuje srovnání dvou biometrických šablon, přičemž se obvykle předpokládá, že patří téže osobě. Dvě biometrické šablony se porovnají, aby se zjistilo, zda osoba uvedená na obou obrázcích je tatáž osoba. Tento postup se používá například při automatizované hraniční kontrole (ABC), která se používá pro hraniční kontroly na letištích.

[57] Například pro lidskou důstojnost. Stejně tak práva na respektování soukromého života a ochranu osobních údajů jsou stěžejní základní práva, která mohou být při používání technologie rozpoznávání obličeje ohrožena. Potenciální dopady se mohou vyskytnout rovněž, pokud jde o nediskriminaci a práva zvláštních skupin, jako jsou děti, starší osoby a osoby se zdravotním postižením. Kromě toho nesmí být používáním této technologie omezována svoboda projevu, sdružování a shromažďování. Viz technologie rozpoznávání obličeje: úvahy o základních právech v souvislosti s prosazováním práva, https://fra.europa.eu/en/publication/2019/facial-recognition.

[58] Ustanovení článku 9 nařízení o ochraně osobních údajů a článku 10 směrnice o prosazování práva. Viz také článek 10 nařízení (EU) 2018/1725 (použitelný pro orgány a instituce EU).

Podle právních předpisů EU týkajících se odpovědnosti za výrobky se odpovědnost za vadné výrobky přičítá výrobci, aniž jsou dotčeny vnitrostátní právní předpisy, které mohou rovněž umožnit přiznání nároku na náhradu od jiných stran.

Zadruhé vyvstává otázka zeměpisného rozsahu legislativního zásahu. Podle názoru Komise je nanejvýš důležité, aby se požadavky vztahovaly na všechny příslušné hospodářské subjekty poskytující produkty nebo služby založené na umělé inteligenci v EU bez ohledu na to, zda jsou usazeny v EU či nikoli. Jinak by cíle legislativního zásahu uvedené výše nemohly být zcela splněny.

F. DODRŽOVÁNÍ A PROSAZOVÁNÍ PRÁVNÍCH PŘEDPISŮ

Pro zajištění toho, aby umělá inteligence byla důvěryhodná a bezpečná a s ohledem na evropské hodnoty a pravidla, musí být platné právní požadavky v praxi dodržovány a účinně prosazovány jak příslušnými vnitrostátními a evropskými orgány, tak dotčenými stranami. Příslušné orgány by měly být schopny prošetřit jednotlivé případy, ale také posoudit dopad na společnost.

Vzhledem k vysokému riziku, jež některé aplikace umělé inteligence pro občany a naši společnost představují (viz oddíl A výše), se Komise v této fázi domnívá, že by bylo zapotřebí objektivní předběžné posouzení shody, aby se ověřilo a zajistilo, že některé z výše uvedených povinných požadavků vztahujících se na vysoce rizikové aplikace (viz oddíl D výše) jsou splněny. Předběžné posouzení shody by mohlo zahrnovat postupy pro testování, inspekci nebo certifikaci[59]. Dále kontroly algoritmů a souborů dat používaných ve fázi vývoje.

Posuzování shody u vysoce rizikových aplikací umělé inteligence by mělo být součástí mechanismů posuzování shody, které již existují u velkého počtu výrobků uváděných na vnitřní trh EU. V případě, že žádný z těchto stávajících mechanismů nebude možné využít, může být nutné zavést podobné mechanismy, které budou vycházet z osvědčených postupů a z možných vstupů zúčastněných stran a evropských organizací pro normalizaci. Každý nový mechanismus by měl být přiměřený a nediskriminační a měl by být založen na transparentních a objektivních kritériích v souladu s mezinárodními závazky.

Při vyvíjení a zavádění systému podléhajícího předběžnému posouzení shody by měly být zohledněny zejména tyto prvky:

- Ne všechny výše uvedené požadavky musí být vhodné ověřovat předběžným posouzením shody. Například požadavek na informace, které mají být poskytovány obecně, není vhodné ověřovat prostřednictvím tohoto posouzení.

- Je třeba zejména zohlednit možnost, že některé systémy umělé inteligence se vyvíjejí a učí na základě zkušeností, což může vyžadovat opakovaná hodnocení po celé období jejich životnosti.

- Potřebu ověřit údaje používané pro účely trénování a příslušné metody programování a trénování, procesy a techniky používané k vytváření, testování a validaci systémů umělé inteligence.

[59]Systém by vycházel z postupů posuzování shody v EU, viz rozhodnutí 768/2008/ES nebo nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti), s přihlédnutím ke zvláštnostem umělé inteligence. Viz „Modrá příručka“ k provádění pravidel EU pro výrobky, 2014.

- V případě, že z posouzení shody vyplyne, že systém umělé inteligence nesplňuje požadavky týkající se například dat používaných pro jeho trénování, budou zjištěné nedostatky muset být napraveny, například změnou v trénování systému v EU takovým způsobem, aby bylo zajištěno splnění všech platných požadavků.

Posouzení shody by bylo povinné pro všechny hospodářské subjekty, jichž se požadavky týkají, bez ohledu na to, kde jsou usazeny[60]. S cílem omezit zátěž malých a středních podniků lze uvažovat o určité podpůrné struktuře, a to i prostřednictvím center pro digitální inovace. Dodržování požadavků by navíc mohly usnadnit normy i specializované online nástroje.

Jakýmkoli předchozím posouzením shody by nemělo být dotčeno sledování dodržování předpisů a prosazování *ex post* příslušnými vnitrostátními orgány. To platí pro vysoce rizikové aplikace umělé inteligence, ale i pro jiné aplikace umělé inteligence podléhající právním požadavkům, ačkoli vysoce riziková povaha dotčených aplikací může být důvodem k tomu, aby jim příslušné vnitrostátní orgány věnovaly zvláštní pozornost. Kontroly *ex post* by měla umožňovat odpovídající dokumentace příslušných aplikací umělé inteligence (viz oddíl E výše) a v příslušných případech by měla existovat možnost, aby třetí strany, jako např. příslušné orgány, takové aplikace testovaly. To může být zvláště důležité v případě, kdy v oblasti základních práv vznikají rizika, která závisí na okolnostech. Takové sledování souladu by mělo být součástí systému průběžného dozoru nad trhem. Aspekty souvisejícími se správou se dále zabývá oddíl H níže.

Kromě toho by jak pro vysoce rizikové aplikace, tak pro další aplikace umělé inteligence měla být zajištěna účinná soudní ochrana pro strany, na něž měly systémy umělé inteligence negativní dopad. Otázky týkající se odpovědnosti dále řeší zpráva o rámci pro bezpečnost a odpovědnost připojená k této bílé knize.

G. DOBROVOLNÉ OZNAČOVÁNÍ APLIKACÍ UMĚLÉ INTELIGENCE, KTERÉ NEJSOU VYSOCE RIZIKOVÉ

Pro aplikace umělé inteligence, které se nepovažují za „vysoce rizikové“ (viz oddíl C výše) a které proto nepodléhají výše uvedeným povinným požadavkům (viz oddíly D, E a F výše), by bylo vedle platných právních předpisů možné zavést dobrovolný systém označování.

V rámci tohoto systému by se zúčastněné hospodářské subjekty, na něž se povinné požadavky nevztahují, mohly rozhodnout buď pro dobrovolné dodržování těchto požadavků, nebo pro určitý soubor obdobných požadavků stanovených zejména pro účely dobrovolného systému. Dotčeným hospodářským subjektům by pak pro jejich aplikace umělé inteligence byla udělena značka kvality.

Dobrovolná značka by dotčeným hospodářským subjektům umožnila signalizovat, že jejich produkty a služby založené na umělé inteligenci jsou důvěryhodné. Pro uživatele by tak bylo snadno rozpoznatelné, že dané produkty a služby jsou v souladu s určitými objektivními a standardizovanými referenčními hodnotami pro celou EU, které přesahují běžně použitelné právní povinnosti, což by pomohlo zvýšit jejich důvěru v systémy umělé inteligence a celkově podpořit využití této technologie.

Tato možnost by znamenala vytvoření nového právního nástroje, který by stanovil dobrovolný rámec pro označování vývojářů a/nebo provozovatelů systémů umělé inteligence, které nejsou považovány za vysoce rizikové. I když by účast na systému označování byla dobrovolná, jakmile by se vývojář nebo provozovatel rozhodl označení používat, požadavky by byly závazné. Kombinace prosazování *ex ante* a *ex post* by musela zajistit splnění všech požadavků.

[60] Pokud jde o příslušnou strukturu řízení, včetně orgánů určených k provádění posouzení shody, viz oddíl H níže.

H. SPRÁVA

Aby se zabránilo roztříštěnosti odpovědnosti, zvýšila kapacita v členských státech a zajistilo se, že Evropa bude postupně vybavena kapacitou potřebnou pro testování a certifikaci produktů a služeb založených na umělé inteligenci, je potřebná evropská správní struktura v oblasti umělé inteligence, která by měla podobu rámce pro spolupráci příslušných vnitrostátních orgánů. V této souvislosti by bylo přínosné podporovat příslušné vnitrostátní orgány, aby mohly plnit svůj mandát v případech, kdy je umělá inteligence využívána.

Evropská řídicí struktura by mohla mít řadu úkolů, mohla by být fórem pro pravidelnou výměnu informací a osvědčených postupů, určování nových trendů, poradenství v oblasti normalizační činnosti a vydávání osvědčení. Měla by rovněž hrát klíčovou úlohu při podpoře provádění právního rámce, například vydáváním pokynů, stanovisek a odborných znalostí. Pro tyto účely by se měla opírat o síť vnitrostátních orgánů i odvětvových sítí a regulačních orgánů na vnitrostátní úrovni i na úrovni EU. Kromě toho by mohl Komisi poskytovat pomoc výbor složený z odborníků.

Řídicí struktura by měla zaručit maximální účast zúčastněných stran. Zúčastněné strany – organizace spotřebitelů a sociální partneři, podniky, výzkumní pracovníci a organizace občanské společnosti – by měli být konzultováni ohledně provádění a dalšího rozvoje tohoto rámce.

Vzhledem k již existujícím strukturám v oblastech, jako jsou finance, léčivé přípravky, letectví, zdravotnické prostředky, ochrana spotřebitele, ochrana údajů, by navrhovaná řídicí struktura neměla zdvojovat stávající funkce. Měla by místo toho navázat úzké vztahy s ostatními příslušnými orgány EU a členských států v různých odvětvích s cílem doplnit stávající odborné znalosti a pomáhat stávajícím orgánům při sledování a dohledu nad činnostmi hospodářských subjektů, které se podílejí na systémech umělé inteligence a produktech a službách s využitím umělé inteligence.

A konečně, pokud bude tato možnost zvolena, provádění posuzování shody by mohlo být svěřeno oznámeným subjektům určeným členskými státy. Testovací centra by měla umožnit nezávislý audit a hodnocení systémů umělé inteligence v souladu s výše uvedenými požadavky. Nezávislé hodnocení posílí důvěru a zajistí objektivitu. Mohlo by rovněž usnadnit práci příslušných odpovědných orgánů.

EU má vynikající testovací a hodnotící centra a měla by rozvíjet svou kapacitu i v oblasti umělé inteligence. Hospodářské subjekty usazené ve třetích zemích, které chtějí vstoupit na vnitřní trh, by mohly využívat určené orgány usazené v EU, nebo – s výhradou dohod o vzájemném uznávání se třetími zeměmi – využívat subjekty ze třetích zemí určených k provádění tohoto hodnocení.

Řídicí struktura související s umělou inteligencí a případná posouzení shody by neměly vliv na pravomoci a povinnosti příslušných orgánů vyplývající ze stávajícího práva Unie v konkrétních odvětvích nebo záležitostech (jako jsou finance, léčivé přípravky, letectví, zdravotnické prostředky, ochrana spotřebitele, ochrana údajů atd.).

6. ZÁVĚR

Umělá inteligence je strategickou technologií, která nabízí mnoho výhod pro občany, společnosti a společnost jako celek, a to za předpokladu, že bude zaměřena na člověka, etická, udržitelná a bude respektovat základní práva a hodnoty. Umělá inteligence nabízí významné zvýšení účinnosti a produktivity, které může posílit konkurenceschopnost evropského průmyslu a zlepšit životní podmínky občanů. Může rovněž přispět k nalezení řešení některých nejnaléhavějších společenských výzev, včetně boje proti změně klimatu a zhoršování stavu životního prostředí, problémů spojených s udržitelností a demografickými změnami a ochranou našich demokracií a v nutných a přiměřených případech i k boji proti trestné činnosti.

Aby Evropa plně využila příležitostí, které umělá inteligence nabízí, musí rozvíjet a posilovat nezbytné průmyslové a technologické kapacity. Jak je uvedeno v doprovodné Evropské strategii pro data, budou nutná také opatření, která umožní, aby se EU stala globálním centrem dat.

Cílem evropského přístupu v oblasti umělé inteligence je podpořit inovační kapacitu Evropy v oblasti umělé inteligence a zároveň podpořit rozvoj a zavádění etické a důvěryhodné umělé inteligence v celé ekonomice EU. Umělá inteligence by měla pracovat ve prospěch lidí a měla by být pozitivní silou pro dobro společnosti.

V této bílé knize a v doprovodné zprávě o rámci pro bezpečnost a odpovědnost Komise zahajuje širokou konzultaci s občanskou společností, průmyslem a akademickými pracovníky z členských států o konkrétních návrzích týkajících se evropského přístupu k umělé inteligenci. Patří sem jak politické prostředky na podporu investic do výzkumu a inovací, posílení rozvoje dovedností a podpora zavádění umělé inteligence ze strany malých a středních podniků, tak návrhy klíčových prvků budoucího regulačního rámce. Tato konzultace umožní komplexní dialog se všemi zúčastněnými stranami, který bude inspirovat Komisi k dalším krokům.

Komise vyzývá k předložení připomínek k návrhům uvedeným v bílé knize prostřednictvím otevřené veřejné konzultace, která je přístupná na adrese https://ec.europa.eu/info/consultations_cs. Připomínky v rámci konzultace je možné zasílat do 19. května 2020.

V rámci běžné praxe Komise odpovědi získané v rámci veřejné konzultace zveřejňuje. Nicméně je možné požádat o zachování důvěrnosti jednotlivých příspěvků nebo jejich částí. V takovém případě uveďte jasně na přední straně, že váš příspěvek nemá být zveřejněn, a zašlete Komisi rovněž nedůvěrnou verzi příspěvku, která bude zveřejněna.