EURÓPSKA
KOMISIA

V Bruseli 19. 2. 2020
COM(2020) 65 final

BIELA KNIHA

o umelej inteligencii – európsky prístup k excelentnosti a dôvere

Biela kniha o umelej inteligencii
Európsky prístup k excelentnosti a dôvere

Umelá inteligencia rýchlo napreduje a bude meniť náš život – či už zlepšovaním zdravotnej starostlivosti (napr. vďaka presnejšej diagnostike či lepšej prevencii chorôb), zefektívňovaním poľnohospodárstva, prispievaním k zmierňovaniu zmeny klímy a adaptácii na ňu, zefektívňovaním výrobných systémov vďaka prediktívnej údržbe, zvyšovaním bezpečnosti Európanov alebo mnohými inými spôsobmi, ktoré si zatiaľ vieme len sotva predstaviť. Umelá inteligencia však zároveň prináša viacero potenciálnych rizík, ako je nepriehľadné rozhodovanie, diskriminácia na základe pohlavia alebo iných charakteristík, zasahovanie do nášho súkromného života či zneužívanie na trestnú činnosť.

V kontexte intenzívnej celosvetovej hospodárskej súťaže potrebujeme spoľahlivý európsky prístup, ktorý bude vychádzať z európskej stratégie pre umelú inteligenciu prezentovanej v apríli 2018[1]. Ak si má EÚ poradiť s príležitosťami a výzvami umelej inteligencie, musí konať jednotne a pri podpore vývoja a zavádzania umelej inteligencie si musí vymedziť vlastnú cestu založenú na európskych hodnotách.

Komisia je odhodlaná vytvárať podmienky na prelomové vedecké úspechy, zachovať vedúce postavenie EÚ v oblasti technológií a zabezpečiť, aby nové technológie slúžili všetkým Európanom – aby zlepšovali ich život a zároveň rešpektovali ich práva.

Predsedníčka Komisie Ursula von der Leyenová vo svojich politických usmerneniach[2] predostrela koordinovaný európsky prístup k ľudským a etickým dôsledkom umelej inteligencie, ako aj úvahy o lepšom využívaní veľkých dát na inovačné účely.

Komisia teda podporuje regulačný a investičný prístup, ktorý má dvojaký cieľ: nabádať k využívaniu umelej inteligencie a zároveň riešiť riziká spojené s niektorými použitiami tejto novej technológie. Účelom tejto bielej knihy je opísať politické možnosti na dosiahnutie spomínaných cieľov. Dokument sa nezaoberá rozvojom a používaním umelej inteligencie na vojenské účely. Komisia vyzýva členské štáty, ostatné európske inštitúcie a všetky zainteresované strany vrátane priemyslu, sociálnych partnerov, organizácií občianskej spoločnosti, výskumníkov, širokej verejnosti a všetkých zainteresovaných strán, aby reagovali na možnosti predostreté nižšie a prispeli k budúcemu rozhodovaniu Komisie v tejto oblasti.

1. ÚVOD

Keďže digitálne technológie sú čoraz dôležitejšou súčasťou každého aspektu ľudského života, občania by im mali dôverovať. Dôveryhodnosť je predpokladom ich prijatia. Pre Európu sa tak otvára príležitosť – jednak vzhľadom na jej silnú oddanosť hodnotám a zásadám právneho štátu, jednak vzhľadom na jej preukázateľnú schopnosť vyvíjať bezpečné, spoľahlivé a sofistikované produkty a služby od letectva až po energetické, automobilové a zdravotnícke zariadenia.

Súčasný a budúci udržateľný hospodársky rast a blahobyt spoločnosti v Európe čoraz viac závisí od hodnoty vytvorenej pomocou údajov. Umelá inteligencia je jednou z najvýznamnejších aplikácií dátového hospodárstva. V súčasnosti je väčšina údajov spojená so spotrebiteľmi a uchováva sa a spracúva v centrálnej cloudovej infraštruktúre. Oproti tomu v budúcnosti bude veľká časť oveľa

[1] Umelá inteligencia pre Európu, COM(2018) 237 final.
[2] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_sk.pdf.

rozsiahlejšieho objemu údajov pochádzať z priemyslu, podnikov a verejného sektora a bude sa ukladať v rôznych systémoch, najmä na výpočtových zariadeniach fungujúcich na okraji siete. Naskytajú sa tak nové príležitosti pre Európu, ktorá má silné postavenie v digitalizovanom priemysle a v medzipodnikových aplikáciách, ale zaostáva v spotrebiteľských platformách.

Jednoducho povedané, umelá inteligencia je skupina technológií, ktoré kombinujú údaje, algoritmy a výpočtovú kapacitu. Pokrok vo výpočtovej technike a zvyšovanie dostupnosti údajov sú preto kľúčovými hybnými silami súčasného rozmachu umelej inteligencie. Európa môže skombinovať svoje silné stránky v oblasti technológií a priemyslu s vysokou kvalitou digitálnej infraštruktúry a regulačným rámcom založeným na jej základných hodnotách, aby **sa stala celosvetovým lídrom v inováciách na poli dátového hospodárstva a jeho aplikácií**, ako sa uvádza v európskej dátovej stratégii[3]. Na tomto základe môže vytvoriť ekosystém umelej inteligencie, vďaka ktorému bude z technológií ťažiť celá európska spoločnosť a hospodárstvo:

- v prospech **občanov**, aby mohli využívať nové výhody, napríklad lepšiu zdravotnú starostlivosť, menej porúch domácich spotrebičov, bezpečnejšie a čistejšie dopravné systémy, lepšie verejné služby,
- v prospech rozvoja **podnikania**, napríklad vďaka novej generácii výrobkov a služieb v oblastiach, kde je Európa mimoriadne silná (strojárstvo, doprava, kybernetická bezpečnosť, poľnohospodárstvo, zelené a obehové hospodárstvo, zdravotná starostlivosť či odvetvia s vysokou pridanou hodnotou, ako je móda či cestovný ruch), a
- v prospech **služieb verejného záujmu**, napríklad vďaka zníženiu nákladov na poskytovanie služieb (doprava, vzdelávanie, energetika a nakladanie s odpadom) zlepšením udržateľnosti výrobkov[4] a poskytnutím vhodných nástrojov orgánom presadzovania práva[5], aby mohli chrániť občanov, a to s náležitými zárukami dodržiavania ich práv a slobôd.

Vzhľadom na možný veľký vplyv umelej inteligencie na našu spoločnosť sa musí európska umelá inteligencia opierať o naše hodnoty a základné práva, ako je ľudská dôstojnosť a ochrana súkromia.

Okrem toho by sa mal vplyv systémov umelej inteligencie posudzovať nielen z pohľadu jednotlivca, ale aj z pohľadu spoločnosti ako celku. Využívanie systémov umelej inteligencie môže zohrávať významnú úlohu pri dosahovaní cieľov udržateľného rozvoja a pri podpore demokratického procesu a sociálnych práv. Európa je vďaka svojim nedávnym návrhom o európskej zelenej dohode[6] lídrom na ceste k riešeniu klimatických a environmentálnych výziev. Digitálne technológie, ako je umelá inteligencia, sú kľúčovým faktorom umožňujúcim dosiahnutie cieľov zelenej dohody. Vzhľadom na rastúci význam umelej inteligencie treba náležite zohľadniť vplyv systémov umelej inteligencie na životné prostredie počas celého ich životného cyklu a pozdĺž celého dodávateľského reťazca, napríklad pokiaľ ide o využívanie zdrojov na trénovanie algoritmov a uchovávanie údajov.

---

[3] COM(2020) 66 final.

[4] Umelá inteligencia a digitalizácia sú vo všeobecnosti zásadnými faktormi, ktoré umožňujú napĺňať ambície Európy vychádzajúce z európskej zelenej dohody. Súčasná environmentálna stopa odvetvia IKT sa však odhaduje na viac ako 2 % všetkých celosvetových emisií. Európska digitálna stratégia, ktorá je súčasťou tejto bielej knihy, navrhuje ekologické transformačné opatrenia pre digitálnu oblasť.

[5] Nástroje umelej inteligencie môžu predstavovať príležitosť na lepšiu ochranu občanov EÚ pred trestnou činnosťou a terorizmom.
Takéto nástroje by mohli napríklad pomôcť identifikovať teroristickú propagandu na internete, odhaliť podozrivé transakcie pri predaji nebezpečných výrobkov, identifikovať nebezpečné skryté predmety alebo nezákonné látky či produkty, poskytnúť pomoc občanom v núdzových situáciách a pomôcť usmerniť špecialistov prvého zásahu.

[6] COM(2019) 640 final.

Na dosiahnutie dostatočného rozsahu a zabránenie fragmentácii jednotného trhu je potrebný spoločný európsky prístup k umelej inteligencii. Zavedenie iniciatív v jednotlivých členských štátoch by mohlo ohroziť právnu istotu, oslabiť dôveru občanov a zabrániť vzniku dynamického európskeho priemyslu.

Táto biela kniha opisuje politické možnosti, ktoré by prispeli k dôveryhodnému a bezpečnému vývoju umelej inteligencie v Európe pri plnom rešpektovaní hodnôt a práv občanov EÚ. Hlavné stavebné prvky tejto bielej knihy sú:

- politický rámec, ktorý stanovuje opatrenia v záujme súčinnosti na európskej, celoštátnej aj regionálnej úrovni. Tento rámec stavia na partnerstve medzi súkromným a verejným sektorom a jeho cieľom je mobilizovať zdroje na dosiahnutie **„ekosystému excelentnosti“** v celom hodnotovom reťazci počnúc výskumom a inováciou a vytvoriť správne stimuly na urýchlenie prijímania riešení založených na umelej inteligencii vrátane prostredia malých a stredných podnikov (MSP),
- kľúčové prvky budúceho regulačného rámca pre umelú inteligenciu v Európe, ktorý vytvorí jedinečný **„ekosystém dôvery“**. Na tento účel musí rámec zabezpečiť súlad s pravidlami EÚ vrátane ochrany základných práv a práv spotrebiteľov, najmä v prípade systémov umelej inteligencie prevádzkovaných v EÚ, ktoré predstavujú vysoké riziko[7]. Stavať na ekosystéme dôvery je politický cieľ ako taký. Občanom by mal dodať odvahu využívať aplikácie umelej inteligencie a podnikom a verejným organizáciám zasa právnu istotu, aby mohli inovovať pomocou umelej inteligencie. Komisia silne podporuje prístup zameraný na ľudí, ktorý bude vychádzať z oznámenia o budovaní dôvery v umelú inteligenciu sústredenú na človeka[8], a zohľadní aj informácie získané v pilotnej fáze etických usmernení, ktoré vypracovala expertná skupina na vysokej úrovni pre umelú inteligenciu.

Európska dátová stratégia, ktorá je sprievodným dokumentom k tejto bielej knihe, má za cieľ umožniť Európe stať sa najatraktívnejším, najbezpečnejším a najdynamickejším dátovo agilným hospodárstvom. Európa tak bude mať k dispozícii tie správne dáta na zlepšenie rozhodnutí a skvalitnenie života všetkých jej občanov. V stratégii sa stanovuje niekoľko politických opatrení vrátane mobilizácie súkromných a verejných investícií potrebných na dosiahnutie tohto cieľa. Napokon treba spomenúť aj analýzu dôsledkov umelej inteligencie, internetu vecí a iných digitálnych technológií pre právne predpisy v oblasti bezpečnosti a zodpovednosti, ktorá sa prezentuje v správe Komisie sprevádzajúcej túto bielu knihu.

2. VYUŽITIE SILNÝCH STRÁNOK PRIEMYSELNÝCH A ODBORNÝCH TRHOV

Európa má dobrú východiskovú pozíciu, aby mohla zúročovať potenciál umelej inteligencie nielen ako používateľ, ale aj ako tvorca a výrobca tejto technológie. Má vynikajúce výskumné strediská, inovačné startupy a popredné svetové postavenie v robotike a konkurencieschopných sektoroch spracovateľského priemyslu a služieb – od automobilového priemyslu cez zdravotnú starostlivosť a energetiku až po finančné služby a poľnohospodárstvo. Vybudovala silnú infraštruktúru výpočtovej kapacity (napr. vysokovýkonné počítače), ktorá je nevyhnutná na fungovanie umelej inteligencie. Európa takisto disponuje veľkými objemami verejných a priemyselných dát, ktorých potenciál sa v súčasnosti dostatočne nevyužíva. Jej priemysel má uznávané prednosti v oblasti bezpečných

[7] Hoci možno bude treba zaviesť ďalšie opatrenia na predchádzanie zneužívaniu umelej inteligencie na kriminálne účely a boj proti nemu, táto problematika nepatrí do rozsahu pôsobnosti tejto bielej knihy.

[8] COM(2019) 168.

a zabezpečených digitálnych systémov s nízkou spotrebou energie, ktoré sú potrebné na ďalší vývoj umelej inteligencie.

Využitie schopnosti EÚ investovať do technológií a infraštruktúr novej generácie, ale aj do digitálnych kompetencií, ako je dátová gramotnosť, zvýši technologickú suverenitu Európy na poli kľúčových podporných technológií a infraštruktúr pre dátové hospodárstvo. Infraštruktúra by mala podporovať vytváranie európskych dátových zásobníkov umožňujúcich dôveryhodnú umelú inteligenciu, teda umelú inteligenciu založenú na európskych hodnotách a pravidlách.

Európa by mala využiť svoje prednosti na posilnenie svojej pozície v ekosystémoch a pozdĺž hodnotového reťazca, od určitých sektorov výroby hardvéru cez softvér až po služby. To sa už v určitom rozsahu deje. Európa vyrába viac než štvrtinu všetkých priemyselných a profesionálnych obslužných robotov (napr. pre precízne poľnohospodárstvo, bezpečnosť, zdravie, logistiku) a zohráva dôležitú úlohu pri vývoji a využívaní softvérových aplikácií pre spoločnosti a organizácie [medzipodnikové aplikácie ako systém plánovania podnikových zdrojov (ERP – Enterprise Resource Planning), projektovacie a inžinierske softvéry], ako aj pri aplikáciách na podporu elektronickej verejnej správy a „inteligentných podnikov“.

Európa má vedúce postavenie pri zavádzaní umelej inteligencie v spracovateľskom priemysle. Viac ako polovica jej najvýznamnejších výrobcov zavádza do svojich výrobných operácií aspoň jeden aspekt umelej inteligencie[9].

Jedným z dôvodov silného postavenia Európy vo výskume je program financovania EÚ, ktorý sa osvedčil ako nápomocný pri združovaní úsilia, predchádzaní duplicite a stimulácii verejných a súkromných investícií v členských štátoch. Za posledné tri roky finančné prostriedky EÚ určené na výskum a inovácie v oblasti umelej inteligencie narástli na 1,5 miliardy EUR, čo predstavuje zvýšenie o 70 % v porovnaní s predchádzajúcim obdobím.

Investície do výskumu a inovácií v Európe však stále predstavujú zlomok verejných a súkromných investícií v iných regiónoch sveta. V roku 2016 sa v Európe do umelej inteligencie investovalo približne 3,2 miliardy EUR v porovnaní s približne 12,1 miliardy EUR v Severnej Amerike a 6,5 miliardy EUR v Ázii[10]. Európa preto musí objem svojich investícií výrazne zvýšiť. Koordinovaný plán v oblasti umelej inteligencie[11] vypracovaný spolu s členskými štátmi sa ukázal ako neoceniteľný pri budovaní užšej spolupráce v oblasti umelej inteligencie v Európe a pri vytváraní synergií v záujme maximalizácie investícií do hodnotového reťazca umelej inteligencie.

3. VYUŽITIE BUDÚCICH PRÍLEŽITOSTÍ: ĎALŠIA VLNA ÚDAJOV

Európa v súčasnosti síce zaostáva v spotrebiteľských aplikáciách a online platformách, čo má za následok konkurenčnú nevýhodu v prístupe k údajom, ale už dochádza k dôležitým zmenám, pokiaľ ide o hodnotu a opakované použitie údajov v rozličných sektoroch. Objem vyprodukovaných údajov na svete rýchlo rastie, pričom sa očakáva nárast z 33 zettabajtov v roku 2018 na 175 zettabajtov v roku 2025.[12] Každá nová vlna údajov je pre Európu príležitosťou vydobyť si svoju pozíciu v dátovo agilnom hospodárstve a stať sa v tejto oblasti svetovým lídrom. Navyše sa v nasledujúcich piatich rokoch dramaticky zmení spôsob, akým sa budú údaje uchovávať a spracúvať. Až 80 % činností spracovania a analýzy údajov, ktoré dnes prebiehajú v cloudoch, sa odohráva v dátových centrách

[9] Nasledujú Japonsko (30 %) a USA (28 %). Zdroj: CapGemini (2019).
[10] 10 kľúčových krokov, ktoré Európa musí prijať v ére umelej inteligencie a automatizácie, McKinsey, 2017).
[11] COM(2018) 795.
[12] IDC (2019).

a centralizovaných výpočtových zariadeniach a 20 % v inteligentných prepojených objektoch, ako sú automobily, domáce spotrebiče alebo výrobné roboty, a vo výpočtových zariadeniach blízko používateľa („edge computing“). Do roku 2025 sa tento pomer výrazne zmení.[13]

Európa je celosvetovým lídrom v nízkovýkonnej elektronike, čo je kľúčové pre ďalšiu generáciu špecializovaných procesorov na účely umelej inteligencie. Na tomto trhu v súčasnosti dominujú subjekty, ktoré sídlia mimo EÚ. Mohlo by sa to zmeniť za pomoci iniciatív, ako je napríklad európska iniciatíva v oblasti procesorov, ktorá sa zaoberá vývojom nízkovýkonných výpočtových systémov pre vysokovýkonnú výpočtovú techniku vrátane edge computingu a systémov ďalšej generácie, alebo pôsobenie spoločného podniku pre kľúčové digitálne technológie, ktorý má začať fungovať v roku 2021. Európa má navyše vedúce postavenie v neuromorfických riešeniach[14], ktoré sú ideálne na automatizáciu priemyselných procesov (priemysel 4.0) a dopravných systémov. Tieto riešenia môžu niekoľkonásobne zlepšiť energetickú efektívnosť.

Najnovší pokrok v oblasti kvantovej výpočtovej techniky umožní exponenciálne zvýšenie kapacity spracovania[15]. Európa môže byť lídrom vo vývoji tejto technológie vďaka svojej akademickej sile v kvantovej výpočtovej technike, ako aj pevnému postaveniu európskeho priemyslu v oblasti kvantových simulátorov a programovacích prostredí pre kvantovú výpočtovú techniku. Európske iniciatívy zamerané na zvýšenie dostupnosti kvantových skúšobných a experimentálnych zariadení pomôžu pri uplatňovaní týchto nových kvantových riešení v rôznych priemyselných a akademických odvetviach.

Európa bude zároveň naďalej na čele pokroku v algoritmických základoch umelej inteligencie, pričom bude vychádzať z vlastnej vedeckej excelentnosti. Treba budovať mosty medzi disciplínami, ktoré momentálne fungujú oddelene, ako sú napríklad strojové učenie a hĺbkové učenie (charakterizované obmedzenou interoperabilitou a potrebou veľkého množstva údajov na trénovanie modelov a učenie sa cez korelácie) či symbolické prístupy (kde sa pravidlá vytvárajú ľudským zásahom). Kombinácia symbolického uvažovania a hĺbkových neurónových sietí nám môže pomôcť lepšie vysvetľovať výsledky v oblasti umelej inteligencie.

4. EKOSYSTÉM EXCELENTNOSTI

Na vybudovanie ekosystému excelentnosti, ktorý môže podporiť vývoj a nasadenie umelej inteligencie v celom hospodárstve a verejnej správe v EÚ, sa musí zintenzívniť činnosť na viacerých úrovniach.

A. SPOLUPRÁCA S ČLENSKÝMI ŠTÁTMI

Komisia ako súčasť svojej stratégie pre umelú inteligenciu prijatej v apríli 2018[16] predstavila v decembri 2018 koordinovaný plán na podporu vývoja a využívania umelej inteligencie v Európe, ktorý vypracovala s členskými štátmi.[17]

V tomto pláne sa navrhuje približne 70 spoločných opatrení zameraných na užšiu a efektívnejšiu spoluprácu medzi členskými štátmi a Komisiou v kľúčových oblastiach, ako sú výskum, investície,

[13] Gartner (2017).
[14] Neuromorfické riešenie je akýkoľvek veľmi rozsiahly systém integrovaných obvodov, ktoré napodobňujú neurobiologické štruktúry prítomné v nervovej sústave.
[15] Kvantové počítače budú mať kapacitu v okamihu spracovať niekoľkonásobne väčšie dátové súbory než tie najvýkonnejšie počítače dneška, čo umožní vývoj nových uplatnení umelej inteligencie vo všetkých sektoroch.
[16] Umelá inteligencia pre Európu, COM(2018) 237.
[17] Koordinovaný plán v oblasti umelej inteligencie, COM(2018) 795.

uplatnenie na trhu, zručnosti a talent, údaje či medzinárodná spolupráca. Plán by mal trvať do roku 2027 a mal by sa pravidelne monitorovať a revidovať.

Cieľom je maximalizovať vplyv investícií do výskumu, inovácií a zavádzania, posudzovať národné stratégie pre umelú inteligenciu a v spolupráci s členskými štátmi budovať na koordinovanom pláne v oblasti umelej inteligencie a rozširovať ho:

- *Opatrenie č. 1: Komisia s prihliadnutím na výsledky verejnej konzultácie o bielej knihe navrhne členským štátom revíziu koordinovaného plánu, ktorá sa má prijať do konca roka 2020.*

Financovanie umelej inteligencie na úrovni EÚ by malo prilákať a sústreďovať investície v oblastiach, v ktorých sa vyžaduje činnosť nad rámec toho, čo by členské štáty dokázali dosiahnuť osamote. Ambíciou je počas nadchádzajúcej dekády získať viac ako 20 miliárd EUR[18] celkových investícií v EÚ v oblasti umelej inteligencie ročne. S cieľom stimulovať súkromné a verejné investície EÚ sprístupní zdroje z programu Digitálna Európa, programu Horizont Európa, ako aj z európskych štrukturálnych a investičných fondov, aby naplnila potreby menej rozvinutých regiónov a vidieckych oblastí.

Koordinovaný plán by mohol byť zameraný aj na spoločenský a environmentálny blahobyt ako na kľúčovú zásadu pri využívaní umelej inteligencie. Systémy umelej inteligencie sú prísľubom riešenia najnaliehavejších problémov vrátane zmeny klímy a zhoršovania životného prostredia. Aj ich samotné fungovanie teda musí byť prijateľné z environmentálneho hľadiska. Umelá inteligencia môže a mala by kriticky posudzovať využívanie zdrojov a spotrebu energie a mala by byť vycvičená tak, aby prijímala rozhodnutia, ktoré sú pozitívne pre životné prostredie. Komisia spoločne s členskými štátmi zváži možnosti podpory a propagácie riešení v oblasti umelej inteligencie, ktoré majú takýto charakter.

B. SÚSTREDENIE ÚSILIA VÝSKUMNÉHO A INOVAČNÉHO SPOLOČENSTVA

Európa si nemôže dovoliť, aby kompetenčné centrá boli aj naďalej rozptýlené, ako je to v súčasnosti. Momentálne totiž žiadne z nich nemá rozsah potrebný na to, aby mohlo konkurovať popredným inštitútom na svete. Je nevyhnutné vytvoriť viac synergií medzi rôznymi európskymi výskumnými centrami umelej inteligencie a zosúladiť ich úsilie o zlepšenie excelentnosti, udržanie a prilákanie najlepších výskumných pracovníkov a vývoj najlepšej technológie. Európa potrebuje hlavné centrum výskumu, inovácií a odborných znalostí, ktoré by toto úsilie koordinovalo, ktoré by bolo celosvetovou uznávanou značkou excelentnosti, pokiaľ ide o umelú inteligenciu, a ktoré by mohlo prilákať investície a najlepšie talenty v tejto oblasti.

Centrá a siete by sa mali sústreďovať do sektorov, v ktorých má Európa potenciál stať sa svetovým lídrom, ako sú priemysel, zdravotníctvo, doprava, financie, agropotravinárske hodnotové reťazce, energetika/životné prostredie, lesníctvo, pozorovanie Zeme a vesmír. Vo všetkých týchto oblastiach prebiehajú preteky o celosvetový prím a Európa ponúka významný potenciál, znalosti a odbornosť[19]. Rovnako dôležité je vytvoriť skúšobné a experimentálne strediská na podporu vývoja a následného zavádzania nových aplikácií umelej inteligencie.

---

[18] COM(2018) 237.

[19] Aj budúci Európsky obranný fond a stála štruktúrovaná spolupráca (PESCO) poskytnú príležitosti na výskum a vývoj v oblasti umelej inteligencie. Tieto projekty by sa mali zosúladiť so širšími civilnými programami EÚ zameranými na umelú inteligenciu.

- *Opatrenie č. 2: Komisia uľahčí vytvorenie centier excelentnosti a skúšobných centier, ktoré budú môcť sústreďovať európske, národné a súkromné investície, a prípadne vypracuje aj nový právny nástroj. Komisia v rámci programu Digitálna Európa navrhla a vyčlenila ambicióznu sumu na podporu svetových referenčných skúšobných centier v Európe. V prípade potreby ju možno doplniť akciami zameranými na výskum a inovácie v rámci programu Horizont Európa ako súčasť viacročného finančného rámca na roky 2021 – 2027.*

C. ZRUČNOSTI

Európsky prístup k umelej inteligencii sa bude musieť opierať o silný dôraz na zručnosti, aby sa doplnili nedostatky v nich[20]. Komisia čoskoro predloží aktualizáciu programu v oblasti zručností, aby všetci v Európe mali prínos z ekologickej a digitálnej transformácie hospodárstva EÚ. Iniciatívy by mohli zahŕňať aj podporu sektorových regulačných orgánov s cieľom zlepšiť ich zručnosti v oblasti umelej inteligencie, aby tak mohli účinne a efektívne vykonávať príslušné pravidlá. Aktualizovaný akčný plán digitálneho vzdelávania pomôže lepšie využívať údaje a technológie založené na umelej inteligencii, ako je vzdelávacia a prognostická analytika, s cieľom skvalitniť systémy vzdelávania a odbornej prípravy a prispôsobiť ich potrebám digitálneho veku. Vďaka plánu sa takisto zvýši informovanosť o umelej inteligencii na všetkých úrovniach vzdelávania, aby občania boli pripravení prijímať fundované rozhodnutia, ktoré umelá inteligencia bude čoraz viac ovplyvňovať.

Rozvoj zručností potrebných na prácu v oblasti umelej inteligencie a zvyšovanie úrovne zručností pracovnej sily na účely transformácie podnietenej umelou inteligenciou bude prioritou revidovaného koordinovaného plánu pre umelú inteligenciu, ktorý sa má vypracovať v spolupráci s členskými štátmi. Mohlo by to zahŕňať premenu hodnotiaceho zoznamu etických usmernení na orientačné „učebné plány“ pre vývojárov umelej inteligencie, ktoré by slúžili ako zdroj pre inštitúcie odbornej prípravy. Malo by sa vyvinúť osobitné úsilie na zvýšenie počtu žien, ktoré sa školia a zamestnávajú v tejto oblasti.

Okrem toho by vlajkové centrum výskumu a inovácií v oblasti umelej inteligencie v Európe vďaka možnostiam, ktoré by ponúkalo, mohlo prilákať talenty z celého sveta. Centrum by navyše rozvíjalo a šírilo excelentnosť v zručnostiach, ktoré by sa rodili a pestovali naprieč Európou.

- *Opatrenie č. 3: Zriadiť a pomocou piliera pokročilých zručností v rámci programu Digitálna Európa podporovať siete popredných univerzít a inštitútov vysokoškolského vzdelávania s cieľom prilákať najlepších profesorov a vedcov a ponúkať špičkové svetové magisterské programy v oblasti umelej inteligencie.*

Okrem potreby zvyšovania úrovne zručností sa pracovníkov a zamestnávateľov priamo týka aj navrhovanie a používanie systémov umelej inteligencie na pracovisku. Zapojenie sociálnych partnerov bude kľúčovým faktorom pri zabezpečovaní toho, aby sa k umelej inteligencii na pracovisku pristupovalo z ľudského hľadiska.

D. DÔRAZ NA MSP

Rovnako bude dôležité zabezpečiť, aby prístup k umelej inteligencii mali MSP a mohli ju využívať. Na tento účel by sa mali ešte viac posilniť centrá digitálnych inovácií[21] a platforma umelej inteligencie

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

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

na požiadanie[22] a mala by sa podporovať spolupráca medzi MSP. Pri dosahovaní tohto cieľa bude kľúčový program Digitálna Európa. Zatiaľ čo MSP by mali pri chápaní a zavádzaní umelej inteligencie pomáhať všetky centrá digitálnych inovácií, bude dôležité, aby aspoň jedno centrum inovácií v každom členskom štáte bolo vysoko špecializované na umelú inteligenciu.

MSP a startupy budú potrebovať prístup k financovaniu, ak majú prispôsobovať svoje procesy alebo inovovať s použitím umelej inteligencie. V nadväznosti na nadchádzajúci pilotný investičný fond v oblasti umelej inteligencie a technológie blockchainu v objeme 100 miliónov EUR Komisia plánuje ďalej rozšíriť prístup k financovaniu v oblasti umelej inteligencie v rámci programu InvestEU[23]. Umelá inteligencia sa výslovne uvádza medzi oprávnenými oblasťami na využitie záruky InvestEU.

- *Opatrenie č. 4: Komisia bude spolupracovať s členskými štátmi na zabezpečení toho, aby aspoň jedno centrum digitálnej inovácie v každom členskom štáte bolo vysoko špecializované na umelú inteligenciu. Centrá digitálnych inovácií možno podporovať v rámci programu Digitálna Európa.*
- *Komisia a Európsky investičný fond v prvom štvrťroku 2020 vyhlásia pilotný projekt v objeme 100 miliónov EUR s cieľom poskytovať kapitálové financovanie inovačného vývoja v oblasti umelej inteligencie. Za predpokladu, že sa dosiahne konečná dohoda o viacročnom finančnom rámci, chce Komisia počnúc rokom 2021 tieto prostriedky výrazne rozšíriť vďaka programu InvestEU.*

E. PARTNERSTVO SO SÚKROMNÝM SEKTOROM

Takisto je dôležité zabezpečiť, aby sa súkromný sektor v plnej miere podieľal na navrhovaní programu v oblasti výskumu a inovácií a aby sa zabezpečila potrebná úroveň spoločných investícií. Vyžaduje si to vytvorenie rozsiahleho verejno-súkromného partnerstva a angažovanosť vrcholového manažmentu spoločností.

- *Opatrenie č. 5: V kontexte programu Horizont Európa Komisia zriadi nové verejno-súkromné partnerstvo v oblasti umelej inteligencie, dát a robotiky s cieľom sústreďovať úsilie, zabezpečiť koordináciu výskumu a inovácií v oblasti umelej inteligencie, spolupracovať s ďalšími verejno-súkromnými partnerstvami v rámci programu Horizont Európa a konať v súčinnosti so skúšobnými zariadeniami a s centrami digitálnych inovácií uvedenými vyššie.*

[22] www.Ai4eu.eu.
[23] https://europa.eu/investeu/.

F. PODPORA ZAVÁDZANIA UMELEJ INTELIGENCIE ZO STRANY VEREJNÉHO SEKTORA

Orgány verejnej správy, nemocnice, verejnoprospešné a dopravné služby, orgány finančného dohľadu a ďalšie oblasti verejného záujmu musia rýchlo začať používať produkty a služby, ktoré využívajú umelú inteligenciu. Osobitný dôraz sa bude klásť na oblasť zdravotníctva a dopravy, kde je technológia pripravená na rozsiahle zavádzanie.

- *Opatrenie č. 6: Komisia začne otvorený a transparentný sektorový dialóg, v ktorom sa bude klásť dôraz najmä na zdravotnú starostlivosť, správne orgány vo vidieckych oblastiach a poskytovateľov služieb verejného záujmu. Cieľom bude predložiť akčný plán na uľahčenie rozvoja, experimentovania a zavádzania. Sektorové dialógy sa použijú na prípravu osobitného programu s názvom Zavádzanie umelej inteligencie, ktorý bude slúžiť na podporu verejného obstarávania systémov umelej inteligencie a ktorý prispeje k transformácii samotných postupov verejného obstarávania.*

G. ZABEZPEČENIE PRÍSTUPU K DÁTOVÝM A POČÍTAČOVÝM INFRAŠTRUKTÚRAM

Oblasti činnosti stanovené v tejto bielej knihe dopĺňajú plán predkladaný súbežne v rámci európskej dátovej stratégie. Zlepšenie prístupu k údajom a ich správy má zásadný význam. Bez údajov nie je možný vývoj umelej inteligencie ani iných digitálnych aplikácií. Obrovské množstvo nových údajov, ktoré ešte len vzniknú, predstavuje príležitosť pre Európu, aby zaujala popredné miesto pri transformácii opierajúcej sa o údaje a umelú inteligenciu. Podpora zodpovedných postupov správy údajov a súladu údajov so zásadami FAIR prispeje k budovaniu dôvery a k zabezpečeniu opätovnej použiteľnosti údajov[24]. Rovnako dôležité sú investície do kľúčových výpočtových technológií a infraštruktúr.

Komisia navrhla v rámci programu Digitálna Európa vyčleniť vyše 4 miliardy EUR na podporu vysokovýkonnej a kvantovej výpočtovej techniky vrátane edge computingu a infraštruktúry založenej na umelej inteligencii, dátovej a cloudovej infraštruktúry. Tieto priority ďalej rozvíja európska dátová stratégia.

H. MEDZINÁRODNÉ ASPEKTY

Európa má dobré postavenie na to, aby mohla zohrávať globálnu vedúcu úlohu pri budovaní partnerstiev v súvislosti so spoločnými hodnotami a podpore etického využívania umelej inteligencie. Práca EÚ v oblasti umelej inteligencie už ovplyvňuje medzinárodné diskusie. Expertná skupina na vysokej úrovni do vypracúvania etických usmernení zapojila viacero organizácií z krajín mimo EÚ a niekoľkých vládnych pozorovateľov. EÚ sa zároveň intenzívne zúčastňovala na rozvoji etických zásad Organizácie pre hospodársku spoluprácu a rozvoj (OECD) týkajúcich sa umelej inteligencie[25]. Skupina G20 následne schválila tieto zásady vo svojom ministerskom vyhlásení o obchode a digitálnom hospodárstve z júna 2019.

EÚ zároveň uznáva, že významné úsilie v oblasti umelej inteligencie prebieha aj na iných multilaterálnych fórach vrátane Rady Európy, Organizácie Spojených národov pre vzdelávanie, vedu a kultúru (UNESCO), OECD, Svetovej obchodnej organizácie a Medzinárodnej telekomunikačnej

[24] Vyhľadateľné, prístupné, interoperabilné a použiteľné (Findable, Accessible, Interoperable and Reusable), ako sa uvádza v záverečnej správe a akčnom pláne expertnej skupiny Komisie pre údaje FAIR, 2018, https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

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

únie (ITU). V rámci OSN sa EÚ zúčastňuje na práci vychádzajúcej zo správy skupiny na vysokej úrovni pre digitálnu spoluprácu vrátane jej odporúčania o umelej inteligencii.

EÚ bude na problematike umelej inteligencie naďalej spolupracovať s podobne zmýšľajúcimi krajinami, ale aj s globálnymi aktérmi. Bude pritom vychádzať z pravidiel a hodnôt EÚ (napr. podpora zbližovania v oblasti regulácie zdola nahor, prístup ku kľúčovým zdrojom vrátane údajov, vytváranie rovnakých podmienok). Komisia bude pozorne monitorovať politiky tretích krajín, ktoré obmedzujú toky údajov, a bude sa zaoberať neprimeranými obmedzeniami jednak v dvojstranných obchodných rokovaniach, jednak prostredníctvom opatrení v kontexte Svetovej obchodnej organizácie. Komisia je presvedčená, že medzinárodná spolupráca v oblasti umelej inteligencie musí byť založená na prístupe, ktorý podporuje rešpektovanie základných práv vrátane ľudskej dôstojnosti, pluralizmu, začleňovania, nediskriminácie a ochrany súkromia a osobných údajov[26], a bude sa usilovať o šírenie svojich hodnôt na celom svete[27]. Takisto je zrejmé, že zodpovedný vývoj a využívanie umelej inteligencie môže byť hnacou silou pri dosahovaní cieľov udržateľného rozvoja a napredovaní v Agende 2030.

5. EKOSYSTÉM DÔVERY: REGULAČNÝ RÁMEC PRE UMELÚ INTELIGENCIU

Podobne ako pri každej novej technológii, aj využívanie umelej inteligencie prináša tak nové príležitosti, ako aj riziká. Občania sa obávajú, že vzhľadom na informačnú asymetriu algoritmického rozhodovania budú bezmocní pri ochrane svojich práv a bezpečnosti. Podniky zasa znepokojuje právna neistota. Hoci umelá inteligencia môže pomôcť chrániť bezpečnosť občanov a umožniť im využívať ich základné práva, verejnosť sa obáva, že táto technológia zároveň môže mať neželaný efekt alebo sa dokonca môže zneužívať. Tieto obavy treba riešiť. Popri nedostatku investícií a zručností je nedôvera navyše jedným z hlavných faktorov, ktoré brzdia širšie využívanie umelej inteligencie.

Komisia preto 25. apríla 2018 vyhlásila stratégiu pre umelú inteligenciu[28], ktorá sa zaoberá sociálno-ekonomickými aspektmi sprevádzajúcimi nárast investícií do výskumu, inovácie a kapacity umelej inteligencie v celej EÚ. Spolu s členskými štátmi schválila koordinovaný plán[29] s cieľom zosúladiť jednotlivé stratégie a navyše zriadila expertnú skupinu na vysokej úrovni, ktorá v apríli 2019 zverejnila usmernenia o dôveryhodnej umelej inteligencii[30].

Komisia uverejnila oznámenie[31], v ktorom víta sedem kľúčových požiadaviek načrtnutých v usmerneniach expertnej skupiny na vysokej úrovni:

- ľudský faktor a dohľad,
- technická spoľahlivosť a bezpečnosť,
- riadenie súkromia a údajov,
- transparentnosť,
- rozmanitosť, nediskriminácia a spravodlivosť,
- spoločenský a environmentálny blahobyt a
- zodpovednosť.

[26] Komisia bude v rámci nástroja partnerstva financovať projekt v hodnote 2,5 milióna EUR, ktorý uľahčí spoluprácu s podobne zmýšľajúcimi partnermi, v záujme podpory etických usmernení EÚ v oblasti umelej inteligencie a prijatia spoločných zásad a operatívnych záverov.

[27] Predsedníčka Von der Leyenová, Ambicióznejšia Únia: Môj plán pre Európu, strana 17.

[28] COM(2018) 237.

[29] COM(2018) 795.

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

[31] COM(2019) 168.

Usmernenia okrem toho obsahujú aj zoznam posúdení, ktorý môžu využiť podniky v praxi. V druhej polovici roka 2019 tento zoznam posúdení otestovalo viac ako 350 organizácií, ktoré zaslali spätnú väzbu. Skupina na vysokej úrovni momentálne reviduje svoje usmernenia so zreteľom na ňu a túto činnosť uzavrie do júna 2020. Kľúčovým výsledkom procesu zhromažďovania spätnej väzby je, že hoci viaceré požiadavky už sú zakotvené v existujúcich právnych alebo regulačných režimoch, platné právne predpisy v mnohých hospodárskych odvetviach zatiaľ osobitne neupravujú aspekty súvisiace s transparentnosťou, vystopovateľnosťou a ľudským dohľadom.

Popri tomto súbore nezáväzných usmernení expertnej skupiny na vysokej úrovni a v súlade s politickými usmerneniami predsedníčky by jasný európsky regulačný rámec upevnil dôveru medzi spotrebiteľmi a podnikmi v oblasti umelej inteligencie, čím by urýchlil zavádzanie tejto technológie. Takýto regulačný rámec by mal zodpovedať ostatným opatreniam na podporu inovačnej kapacity a konkurencieschopnosti Európy v tejto oblasti. Okrem toho musí zabezpečiť sociálne, environmentálne a hospodársky optimálne výsledky a súlad s právnymi predpismi, so zásadami a s hodnotami EÚ. Týka sa to najmä oblastí, v ktorých môžu byť práva občanov najviac dotknuté, napríklad v prípade aplikácii umelej inteligencie na účely presadzovania práva či v súdnictve.

Vývojári a používatelia umelej inteligencie už podliehajú európskym právnym predpisom o základných právach (napr. ochrana údajov, súkromie, nediskriminácia), ochrane spotrebiteľa a bezpečnosti a zodpovednosti výrobkov. Spotrebitelia očakávajú rovnakú úroveň bezpečnosti a rešpektovanie svojich práv bez ohľadu na to, či produkt alebo systém využíva umelú inteligenciu. Uplatňovanie a presadzovanie týchto právnych predpisov však môžu skomplikovať niektoré osobitné vlastnosti umelej inteligencie (napr. nepriehľadnosť). Preto treba preskúmať, či si súčasné právne predpisy dokážu poradiť s rizikami umelej inteligencie a či ich možno účinne presadzovať, či ich treba upraviť alebo či sú potrebné nové predpisy.

Vzhľadom na to, ako rýchlo sa vyvíja umelá inteligencia, musí regulačný rámec ponechať priestor na zohľadnenie ďalšieho vývoja. Akékoľvek zmeny by sa mali obmedziť na jasne identifikované problémy, pre ktoré existujú realistické riešenia.

Členské štáty poukazujú na to, že momentálne chýba spoločný európsky rámec. Nemecká komisia pre etiku údajov vyzvala na vytvorenie päťúrovňového systému regulácie založeného na riziku, ktorý by siahal od nulovej regulácie v prípade najneškodnejších systémov umelej inteligencie až po úplný zákaz v prípade tých najnebezpečnejších. Dánsko nedávno predstavilo značku dátovej etiky a Malta zasa zaviedla dobrovoľný systém certifikácie umelej inteligencie. Ak EÚ nezabezpečí celoúnijný prístup, existuje reálne riziko fragmentácie vnútorného trhu, čo by ohrozilo ciele dôvery, právnej istoty a prenikania na trh.

Spoľahlivý európsky regulačný rámec pre dôveryhodnú umelú inteligenciu bude chrániť všetkých európskych občanov a pomôže vytvoriť bezproblémový vnútorný trh v záujme ďalšieho vývoja a využívania umelej inteligencie, ako aj posilnenia európskej priemyselnej základne v oblasti umelej inteligencie.

A. VYMEDZENIE PROBLÉMU

Hoci umelá inteligencia môže byť veľmi prínosná, napríklad tým, že zvýši bezpečnosť produktov a procesov, môže spôsobiť aj škody. Tie môžu byť materiálne (bezpečnosť a zdravie jednotlivcov vrátane straty na životoch, škody na majetku) alebo nemateriálne (strata súkromia, obmedzovanie práva na slobodu prejavu, ľudská dôstojnosť, diskriminácia napríklad v prístupe k zamestnaniu) a môžu sa týkať širokej škály rizík. Regulačný rámec by sa mal zamerať na to, ako minimalizovať rôzne riziká potenciálnej ujmy, najmä tie najvýznamnejšie.

Hlavné riziká súvisiace s používaním umelej inteligencie sa týkajú uplatňovania pravidiel určených na ochranu základných práv (vrátane ochrany osobných údajov a súkromia a nediskriminácie), ako aj otázok bezpečnosti[32] a zodpovednosti.

Riziká ohrozujúce základné práva vrátane ochrany osobných údajov a súkromia a nediskriminácie

Používanie umelej inteligencie môže mať vplyv na hodnoty, na ktorých je založená EÚ, a viesť k porušovaniu základných práv[33] vrátane práva na slobodu prejavu, slobody zhromažďovania, ľudskej dôstojnosti, nediskriminácie na základe pohlavia, rasy alebo etnického pôvodu, náboženstva alebo viery, zdravotného postihnutia, veku alebo sexuálnej orientácie (v závislosti od oblasti), ochrany osobných údajov a súkromia[34] alebo práva na účinný súdny prostriedok nápravy a spravodlivý proces, ako aj ochrany spotrebiteľa. Tieto riziká môžu vyplývať z nedostatkov v celkovom návrhu systémov umelej inteligencie (vrátane tých, ktoré zahŕňajú ľudský dohľad) alebo z používania údajov bez toho, aby sa odstránila prípadná zaujatosť (napr. systém pri učení využíva len alebo hlavne údaje od mužov, čo vedie k neoptimálnym výsledkom u žien).

Umelá inteligencia môže suplovať mnohé funkcie, ktoré predtým mohli vykonávať len ľudia. Preto budú občanov a právnické osoby čoraz viac ovplyvňovať činnosti a rozhodnutia, ktoré budú prijímať alebo pri ktorých prijímaní budú asistovať systémy umelej inteligencie, čo môže byť niekedy ťažké pochopiť a v prípade potreby proti tomu niečo účinne podniknúť. Umelá inteligencia navyše zvyšuje možnosti sledovania a analyzovania každodenného života ľudí. Existuje napríklad potenciálne riziko, že umelú inteligenciu by v rozpore s ochranou údajov EÚ a inými pravidlami mohli použiť štátne orgány alebo iné subjekty na účely hromadného sledovania alebo zamestnávatelia na monitorovanie správania zamestnancov. Vďaka analýze veľkých objemov údajov a identifikovaniu prepojení medzi nimi sa môže umelá inteligencia použiť aj na spätné vysledovanie a deanonymizáciu údajov o osobách, čím môžu vznikať nové riziká ohrozujúce ochranu osobných údajov, a to aj v prípade dátových súborov, ktoré samy osebe nezahŕňajú osobné údaje. Umelú inteligenciu využívajú aj online sprostredkovatelia na triedenie informácií pre svojich používateľov v závislosti od priority a na úpravu obsahu. Spracúvané údaje, dizajn aplikácií a miera ľudskej intervencie môžu ovplyvniť právo na slobodu prejavu, ochranu osobných údajov, súkromie či politické slobody.

[32] Patria sem otázky kybernetickej bezpečnosti, otázky súvisiace s aplikáciami umelej inteligencie v kritických infraštruktúrach alebo zneužívanie umelej inteligencie.

[33] Z výskumu Rady Európy vyplýva, že používanie umelej inteligencie by mohlo ovplyvniť veľký počet základných práv – https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

[34] Tieto riziká sa riešia vo všeobecnom nariadení o ochrane údajov a v smernici o súkromí a elektronických komunikáciách (o novom nariadení o súkromí a elektronických komunikáciách sa rokuje), ale možno by bolo treba preskúmať, či systémy umelej inteligencie neprinášajú ďalšie hrozby. Komisia bude priebežne monitorovať a posudzovať uplatňovanie všeobecného nariadenia o ochrane údajov.

V určitých algoritmoch umelej inteligencie, napríklad pri predpovedaní recidívy trestného činu, sa môžu objavovať predsudky na základe pohlavia alebo rasy: tieto algoritmy môžu predpovedať odlišnú mieru pravdepodobnosti recidívy u žien v porovnaní s mužmi alebo u domáceho obyvateľstva v porovnaní s cudzincami. *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", Cena za najlepšiu štúdiu, Medzinárodná konferencia o umelej inteligencii a práve, 2019.*

Niektoré programy umelej inteligencie na analýzu tváre vykazujú predpojatosť, pokiaľ ide o pohlavie a rasu – vykazujú nízku chybovosť pri určovaní pohlavia v prípade mužov so svetlejšou pokožkou, ale veľkú chybovosť pri určovaní pohlavia v prípade žien tmavšej pleti. Zdroj: *Joy Buolamwini, Timnit Gebru, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018.*

Predpojatosť a diskriminácia predstavujú inherentné riziká akejkoľvek spoločenskej alebo hospodárskej činnosti. Ľudské rozhodovanie nie je imúnne proti chybám a predsudkom. Rovnaká predpojatosť v systémoch umelej inteligencie by však mohla mať oveľa väčší dosah a mohla by ovplyvňovať a diskriminovať mnohých ľudí, ak by nepodliehala mechanizmom sociálnej kontroly, ktorými sa riadi ľudské správanie[35]. Môže k tomu dochádzať aj vtedy, keď sa systém umelej inteligencie „učí" počas prevádzky. V takýchto prípadoch, keď výsledku nebolo možné zabrániť ani ho predvídať vo fáze návrhu, riziká nebudú vyplývať z chyby pôvodného návrhu systému, ale skôr z praktických vplyvov korelácií alebo vzorcov, ktoré systém identifikuje vo veľkom súbore údajov.

Špecifické charakteristiky mnohých technológií umelej inteligencie vrátane nepriehľadnosti („efekt čiernej skrinky"), komplexnosti, nepredvídateľnosti a čiastočne autonómneho správania môžu sťažiť overovanie dodržiavania pravidiel zakotvených v právnych predpisoch EÚ slúžiacich na ochranu základných práv a brániť účinnému presadzovaniu týchto predpisov. Orgány presadzovania práva a dotknuté osoby by mohli mať nedostatok prostriedkov na preskúmanie toho, ako sa dospelo k určitému rozhodnutiu, pri prijímaní ktorého sa použila umelá inteligencia, a teda či boli dodržané príslušné pravidlá. Jednotlivci a právnické osoby môžu čeliť ťažkostiam s účinným prístupom k spravodlivosti v situáciách, keď ich takéto rozhodnutia môžu negatívne zasiahnuť.

Riziká pre bezpečnosť a účinné fungovanie režimu zodpovednosti

Technológie umelej inteligencie, ktoré sú súčasťou produktov a služieb, môžu pre používateľov predstavovať nové bezpečnostné riziká. Napríklad v dôsledku chyby v technológii rozpoznávania objektov môže autonómne vozidlo nesprávne identifikovať objekt na ceste a spôsobiť nehodu, pri ktorej dôjde k zraneniam a materiálnym škodám. Podobne ako pri rizikách v súvislosti so základnými právami, aj tieto riziká môžu byť spôsobené nedostatkami v návrhu technológie umelej inteligencie, prípadne môžu súvisieť s dostupnosťou a kvalitou údajov alebo s inými problémami vyplývajúcimi zo

[35] Poradný výbor Komisie pre rovnosť príležitostí pre ženy a mužov momentálne pripravuje dokument s názvom Stanovisko k umelej inteligencii, v ktorom okrem iného analyzuje vplyv umelej inteligencie na rodovú rovnosť. Výbor má dokument prijať začiatkom roka 2020. Aj v stratégii EÚ pre rodovú rovnosť na roky 2020 – 2024 sa rieši prepojenie medzi umelou inteligenciou a rodovou rovnosťou. Európska sieť vnútroštátnych orgánov pre otázky rovnosti (Equinet) uverejní správu (autori: Robin Allen a Dee Masters) s názvom Regulácia umelej inteligencie: nová úloha orgánov pre otázky rovnosti – Zvládnutie nových výziev v oblasti rovnosti a nediskriminácie v nadväznosti na rastúcu digitalizáciu a využívanie umelej inteligencie. Očakáva sa začiatkom roka 2020.

strojového učenia. Hoci niektoré z týchto rizík sa neobmedzujú len na výrobky a služby, ktoré sa opierajú o umelú inteligenciu, používanie umelej inteligencie ich môže zvýšiť alebo zhoršiť.

Nedostatok jasných bezpečnostných opatrení na riešenie týchto rizík môže okrem hrozieb pre dotknuté osoby vytvoriť aj právnu neistotu pre podniky, ktoré predávajú produkty využívajúce umelú inteligenciu v EÚ. Orgánom dohľadu nad trhom a orgánom presadzovania práva sa môže stať, že si nebudú isté, či môžu zasiahnuť, pretože nemusia mať právomoci konať a/alebo nemusia mať primerané technické schopnosti na kontrolu systémov[36]. Právna neistota preto môže znížiť celkovú úroveň bezpečnosti a oslabiť konkurencieschopnosť európskych spoločností.

V situáciách, v ktorých sa bezpečnostné riziká naplnia, nedostatok jasných požiadaviek a špecifické črty technológií umelej inteligencie uvedené vyššie sťažujú vystopovanie potenciálne problematických rozhodnutí prijatých so zapojením systémov umelej inteligencie. Osoby, ktoré utrpeli škodu, tak môžu mať ťažkosti so získaním kompenzácie podľa súčasných právnych predpisov EÚ a vnútroštátnych právnych predpisov o zodpovednosti za škodu[37].

Podľa smernice o zodpovednosti za výrobky za škody spôsobené chybným výrobkom zodpovedá výrobca. V prípade systému založeného na umelej inteligencii, ako sú autonómne vozidlá, však môže byť ťažké dokázať, že výrobok je chybný, aká škoda vznikla a aká je príčinná súvislosť medzi nimi. Okrem toho existuje určitá neistota, pokiaľ ide o to, ako a do akej miery sa smernica o zodpovednosti za výrobky uplatňuje v prípade určitých druhov chýb – napríklad ak sú spôsobené slabou kybernetickou bezpečnosťou výrobku.

Preto sa problém spätného vystopovania potenciálne problematických rozhodnutí prijatých systémami umelej inteligencie spomínaný vyššie v súvislosti so základnými právami rovnako vzťahuje aj na otázky bezpečnosti a zodpovednosti. Osoby, ktoré utrpeli škodu, napríklad nemusia mať účinný prístup k dôkazom, ktoré sú potrebné na predloženie prípadu súdnym orgánom, a môžu mať menej efektívne možnosti nápravy v porovnaní so situáciami, keď je škoda spôsobená tradičnými technológiami. Tieto riziká budú s čoraz častejším využívaním umelej inteligencie narastať.

B. MOŽNÉ ÚPRAVY EXISTUJÚCEHO LEGISLATÍVNEHO RÁMCA EÚ V OBLASTI UMELEJ INTELIGENCIE

Na viaceré nové aplikácie umelej inteligencie sa vzťahuje a potenciálne uplatňuje rozsiahly súbor existujúcich právnych predpisov EÚ v oblasti bezpečnosti výrobkov a zodpovednosti[38] vrátane predpisov platných v jednotlivých odvetviach, ktorý je ďalej doplnený vnútroštátnymi právnymi predpismi.

Pokiaľ ide o ochranu základných práv a práv spotrebiteľov, legislatívny rámec EÚ zahŕňa právne predpisy, ako je smernica o rasovej rovnosti[39], smernica o rovnakom zaobchádzaní v zamestnaní

[36] Ako príklad možno uviesť detské inteligentné hodinky. Tento výrobok možno dieťaťu, ktoré ho nosí, nijako priamo neškodí, ale ak sa nezaručí minimálna úroveň bezpečnosti, môže sa ľahko zneužiť ako nástroj na získanie prístupu k dieťaťu. Orgánom dohľadu nad trhom sa môže ťažko zasahovať v prípadoch, keď riziko nie je spojené s výrobkom ako takým.

[37] Spojenie umelej inteligencie, internetu vecí a iných digitálnych technológií s právnymi predpismi v oblasti bezpečnosti a zodpovednosti sa analyzuje v správe Komisie priloženej k tejto bielej knihe.

[38] Právny rámec EÚ pre bezpečnosť výrobkov pozostáva zo smernice o všeobecnej bezpečnosti výrobkov (smernica 2001/95/ES), ktorá predstavuje akúsi bezpečnostnú sieť, a niekoľkých pravidiel špecifických pre jednotlivé odvetvia, ktoré sa vzťahujú na rôzne kategórie výrobkov (od strojov cez lietadlá, automobily a hračky až po zdravotnícke pomôcky) a ktorých cieľom je zaručiť vysokú úroveň ochrany zdravia a bezpečnosti. Právne predpisy týkajúce sa zodpovednosti za výrobky dopĺňajú rôzne systémy občianskoprávnej zodpovednosti za škody spôsobené výrobkami alebo službami.

[39] Smernica 2000/43/ES.

a povolaní[40], smernice o rovnakom zaobchádzaní s mužmi a ženami vo vzťahu k zamestnaniu a prístupu k tovaru a službám[41], viaceré pravidlá na ochranu spotrebiteľa[42], ako aj pravidlá ochrany osobných údajov a súkromia, najmä všeobecné nariadenie o ochrane údajov a iné odvetvové právne predpisy týkajúce sa ochrany osobných údajov, ako je napríklad smernica o presadzovaní práva v oblasti ochrany údajov[43]. Okrem toho sa od roku 2025 budú uplatňovať pravidlá týkajúce sa požiadaviek na prístupnosť výrobkov a služieb stanovené v Európskom akte o prístupnosti[44]. Navyše sa pri vykonávaní iných právnych predpisov EÚ musia dodržiavať základné práva, a to aj v oblasti finančných služieb, migrácie alebo zodpovednosti online sprostredkovateľov.

Hoci právne predpisy EÚ zostávajú v zásade plne uplatniteľné bez ohľadu na zapojenie umelej inteligencie, je dôležité posúdiť, či ich možno primerane presadzovať, ak sa majú riešiť riziká spôsobené systémami umelej inteligencie, alebo či sú potrebné úpravy konkrétnych právnych nástrojov.

Napríklad hospodárske subjekty sú naďalej plne zodpovedné za súlad umelej inteligencie s existujúcimi pravidlami, ktoré chránia spotrebiteľov. Akékoľvek algoritmické využívanie údajov o spotrebiteľskom správaní v rozpore s platnými pravidlami je zakázané a porušenia predpisov sa náležite trestajú.

Komisia sa nazdáva, že legislatívny rámec by sa dal zlepšiť, aby dokázal reagovať na tieto riziká a situácie:

- *Účinné uplatňovanie a presadzovanie existujúcich únijných a vnútroštátnych právnych predpisov:* kľúčové črty umelej inteligencie vytvárajú výzvy súvisiace so zabezpečovaním riadneho uplatňovania a presadzovania únijných a vnútroštátnych právnych predpisov. Nedostatok transparentnosti (nepriehľadnosť umelej inteligencie) sťažuje identifikáciu a dokazovanie možných porušení právnych predpisov vrátane právnych ustanovení, ktoré chránia základné práva, prisudzujú zodpovednosť a vymedzujú podmienky na uplatnenie nároku na náhradu škody. Ak sa teda má zabezpečiť účinné uplatňovanie a presadzovanie, môže byť potrebné upraviť alebo objasniť existujúce právne predpisy v určitých oblastiach, napríklad v súvislosti so zodpovednosťou, ako sa podrobnejšie uvádza v správe, ktorá je priložená k tejto bielej knihe.

- *Obmedzenia rozsahu pôsobnosti existujúcich právnych predpisov EÚ:* právne predpisy EÚ v oblasti bezpečnosti výrobkov sú zamerané najmä na uvádzanie výrobkov na trh. Hoci podľa právnych predpisov EÚ v oblasti bezpečnosti výrobkov softvér, ktorý je súčasťou konečného výrobku, musí spĺňať príslušné pravidlá bezpečnosti výrobkov, je diskutabilné, či sa (okrem určitých odvetví s explicitnými pravidlami[45]) uvedené predpisy vzťahujú aj na samostatný softvér. Aktuálne platné všeobecné právne predpisy EÚ v oblasti bezpečnosti sa uplatňujú na výrobky, a nie na služby, a teda v zásade ani na služby založené na technológiách umelej inteligencie (napr. zdravotnícke, finančné či dopravné služby).

[40] Smernica 2000/78/ES.
[41] Smernica 2004/113/ES, smernica 2006/54/ES.
[42] Napríklad smernica o nekalých obchodných praktikách (smernica 2005/29/ES) a smernica o právach spotrebiteľov (smernica 2011/83/ES).
[43] Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov.
[44] Smernica (EÚ) 2019/882 o požiadavkách na prístupnosť výrobkov a služieb.
[45] Napríklad softvér určený výrobcom na používanie na lekárske účely sa podľa nariadenia o zdravotníckych pomôckach [nariadenie (EÚ) 2017/745] považuje za zdravotnícku pomôcku.

- *Zmena funkčnosti systémov umelej inteligencie:* integrácia softvéru vrátane umelej inteligencie do výrobkov môže zmeniť fungovanie takýchto výrobkov a systémov počas ich životného cyklu. Platí to najmä pre systémy, ktoré si vyžadujú časté aktualizácie softvéru alebo ktoré sa spoliehajú na strojové učenie. Tieto funkcie môžu viesť k vzniku nových rizík, ktoré neboli pri uvedení systému na trh prítomné. Tieto riziká sa v existujúcich právnych predpisoch dostatočne neupravujú, lebo tie sa zameriavajú prevažne na bezpečnostné riziká vyskytujúce sa v čase uvedenia na trh.

- *Neistota v súvislosti s rozdelením zodpovedností medzi rôzne hospodárske subjekty v dodávateľskom reťazci:* právne predpisy EÚ o bezpečnosti výrobkov vo všeobecnosti pripisujú zodpovednosť za výrobok uvedený na trh vrátane všetkých komponentov (napríklad systémov umelej inteligencie) výrobcovi. Tieto pravidlá sa však môžu ukázať ako nejasné napríklad vtedy, ak prvok umelej inteligencie do výrobku pridá po jeho uvedení na trh subjekt, ktorý nie je výrobcom. Právne predpisy EÚ o zodpovednosti za výrobky navyše upravujú iba zodpovednosť výrobcov a zodpovednosť ostatných subjektov v dodávateľskom reťazci ponechávajú na vnútroštátne pravidlá.

- *Zmeny pojmu bezpečnosť:* používanie umelej inteligencie vo výrobkoch a službách môže mať za následok riziká, ktoré právne predpisy EÚ v súčasnosti výslovne neupravujú. Tieto riziká môžu byť spojené s kybernetickými hrozbami, osobno-bezpečnostnými rizikami (spojenými napríklad s novými aplikáciami umelej inteligencie, ako sú domáce spotrebiče), hrozbami vyplývajúcimi zo straty pripojenia atď. Tieto riziká môžu byť prítomné v čase uvádzania výrobkov na trh alebo môžu vzniknúť v dôsledku aktualizácie softvéru alebo samoučenia sa, keď sa výrobok používa. EÚ by mala v plnej miere využívať nástroje, ktoré má k dispozícii, na zozbieranie ďalších dôkazov o potenciálnych rizikách spojených s aplikáciami umelej inteligencie vrátane skúseností Agentúry EÚ pre kybernetickú bezpečnosť (ENISA) s cieľom posúdiť hrozby v oblasti umelej inteligencie.

Ako bolo uvedené, viaceré členské štáty už skúmajú možnosti toho, ako by sa výzvy spojené s umelou inteligenciou dali riešiť vo vnútroštátnych právnych predpisoch. Z toho však vyplýva riziko roztrieštenia jednotného trhu. Rozdielne vnútroštátne pravidlá by mohli vytvoriť prekážky pre spoločnosti, ktoré chcú predávať a prevádzkovať systémy umelej inteligencie na jednotnom trhu. Zaistenie spoločného prístupu na úrovni EÚ by európskym spoločnostiam umožnilo využívať bezproblémový prístup na jednotný trh a podporiť ich konkurencieschopnosť na svetových trhoch.

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

V správe, ktorá sprevádza túto bielu knihu, sa analyzuje príslušný právny rámec. Identifikujú sa v nej prvky neistoty, pokiaľ ide o uplatňovanie tohto rámca so zreteľom na špecifické riziká, ktoré predstavujú systémy umelej inteligencie a iné digitálne technológie.

V správe sa konštatuje, že platné právne predpisy v oblasti bezpečnosti výrobkov už podporujú rozšírený pojem bezpečnosti, ktorým sa zaručuje ochrana pred všetkými druhmi rizík vyplývajúcich z výrobku v závislosti od jeho použitia. V záujme väčšej právnej istoty by sa však mohli zaviesť ustanovenia, ktoré by výslovne menovali nové riziká vyplývajúce z nových digitálnych technológií.

- Autonómne správanie určitých systémov umelej inteligencie počas životného cyklu výrobku môže zahŕňať jeho dôležité zmeny, ktoré majú vplyv na bezpečnosť, čo si môže vyžadovať nové posúdenie rizika. Okrem toho môže byť ako záruka potrebný ľudský dohľad – počnúc fázou navrhovania, ako aj počas celého životného cyklu produktov a systémov umelej inteligencie.
- V prípade potreby by sa mohla zvážiť aj úprava explicitných povinností výrobcov, pokiaľ ide o riziká súvisiace s duševným bezpečím používateľov (napr. spolupráca s humanoidnými robotmi).
- V právnych predpisoch Únie v oblasti bezpečnosti výrobkov by sa mohli stanoviť osobitné požiadavky na riešenie ohrozenia bezpečnosti v súvislosti s chybnými údajmi v štádiu návrhu, ako aj mechanizmy na zaistenie toho, aby sa počas používania produktov a systémov umelej inteligencie zachovala kvalita údajov.
- Nepriehľadnosť systémov založených na algoritmoch by sa mohla riešiť zavedením požiadaviek na transparentnosť.
- Existujúce pravidlá možno bude potrebné upraviť a objasniť v prípade samostatného softvéru, ktorý sa uvádza na trh ako taký alebo sťahuje do výrobku po jeho uvedení na trh, ak má vplyv na bezpečnosť.
- Vzhľadom na rastúcu zložitosť dodávateľských reťazcov, pokiaľ ide o nové technológie, by mohli poskytnúť právnu istotu ustanovenia, ktoré by osobitne vyžadovali spoluprácu medzi hospodárskymi subjektmi v dodávateľskom reťazci a používateľmi.

Vlastnosti nových digitálnych technológií, ako je umelá inteligencia, internet vecí a robotika, môžu otriasť určitými aspektmi rámcov zodpovednosti a mohli by znížiť ich účinnosť. Niektoré z týchto čŕt by mohli spôsobiť, že sa skomplikuje možnosť vystopovať pôvodcu škody, čo by v súlade s väčšinou vnútroštátnych pravidiel bolo potrebné na uplatnenie náhrady škody v dôsledku chyby. To by mohlo výrazne zvýšiť náklady pre poškodených a znamenalo by to, že zodpovednosť od subjektov iných než výrobcov by sa mohla ťažko nárokovať či dokazovať.

- Osoby, ktoré utrpeli ujmu v dôsledku zapojenia systémov umelej inteligencie, musia mať rovnakú úroveň ochrany ako osoby, ktorým škodu spôsobili iné technológie, a to bez toho, aby sa bránilo technologickým inováciám.
- Mali by sa dôkladne posúdiť všetky možnosti na zabezpečenie tohto cieľa – vrátane možných zmien smernice o zodpovednosti za výrobky a možného ďalšieho cieleného zosúladenia vnútroštátnych pravidiel o zodpovednosti. Komisia sa napríklad snaží zozbierať názory na to, či a do akej miery môže byť potrebné zmierniť dôsledky zložitosti prispôsobením dôkazného bremena, ktoré si vyžadujú vnútroštátne pravidlá o zodpovednosti za škody spôsobené prevádzkou aplikácií umelej inteligencie.

Na základe uvedených skutočností Komisia dospela k záveru, že okrem možných úprav existujúcich právnych predpisov môžu byť potrebné nové právne predpisy špecificky zamerané na umelú inteligenciu, aby sa právny rámec EÚ prispôsobil súčasnému a očakávanému technologickému a obchodnému vývoju.

C. ROZSAH PÔSOBNOSTI BUDÚCEHO REGULAČNÉHO RÁMCA EÚ

Kľúčovou otázkou pre budúci špecifický regulačný rámec zameraný na umelú inteligenciu je určiť rozsah jeho uplatňovania. Pracovným predpokladom je, že regulačný rámec by sa vzťahoval na produkty a služby, ktoré sa opierajú o umelú inteligenciu. Umelá inteligencia by preto mala byť jasne vymedzená tak na účely tejto bielej knihy, ako aj na účely prípadnej budúcej politickej iniciatívy.

Komisia prvú definíciu umelej inteligencie predostrela vo svojom oznámení o umelej inteligencii pre Európu[46]. Túto definíciu ďalej zdokonalila expertná skupina na vysokej úrovni[47].

V každom novom právnom nástroji bude musieť byť definícia umelej inteligencie dostatočne flexibilná, aby zohľadňovala technický pokrok, a zároveň dostatočne presná na to, aby poskytla potrebnú právnu istotu.

Na účely tejto bielej knihy, ako aj prípadné budúce diskusie o politických iniciatívach sa zdá dôležité objasniť hlavné prvky, ktoré tvoria umelú inteligenciu – „údaje“ a „algoritmy“. Umelá inteligencia môže byť súčasťou hardvéru. V prípade techník strojového učenia, ktoré tvoria podsúbor umelej inteligencie, sa algoritmy cvičia na súbore údajov, aby dokázali odvodiť určité vzorce a určiť kroky potrebné na dosiahnutie daného cieľa. Algoritmy sa môžu učiť aj počas prevádzky. Hoci produkty založené na umelej inteligencii môžu konať samostatne vďaka tomu, že vnímajú svoje okolie, a to aj bez toho, aby sa riadili vopred stanoveným súborom pokynov, ich správanie vo veľkej miere určujú a obmedzujú ich vývojári. Práve ľudia určujú a programujú ciele, na plnenie ktorých by sa mali systémy umelej inteligencie optimalizovať.

> Pri autonómnej jazde napríklad algoritmus v reálnom čase používa údaje z automobilu (rýchlosť, spotreba motora, tlmiče atď.) a zo snímačov snímajúcich celé okolie vozidla (cesta, značky, iné vozidlá, chodci atď.). Z nich potom odvodzuje, aký smer, zrýchlenie a rýchlosť by malo vozidlo zvoliť, aby sa dostalo do cieľa. Na základe pozorovaných údajov sa algoritmus prispôsobuje situácii na ceste a vonkajším podmienkam vrátane správania iných vodičov, aby zaistil čo najpohodlnejšiu a najbezpečnejšiu jazdu.

EÚ má prísny právny rámec, ktorý okrem iného garantuje ochranu spotrebiteľov, riešenie nekalých obchodných praktík a ochranu osobných údajov a súkromia. Okrem toho *acquis* obsahuje osobitné pravidlá pre určité odvetvia (napr. zdravotníctvo, doprava). Tieto existujúce ustanovenia práva EÚ sa

[46] COM(2018) 237 final, s. 1: „Umelá inteligencia sú systémy, ktoré vykazujú inteligentné správanie tým, že analyzujú okolité prostredie a podnikajú kroky – s istou mierou samostatnosti – na dosiahnutie konkrétnych cieľov. Systémy umelej inteligencie môžu byť založené výlučne na softvéri a pôsobiť vo virtuálnom svete (napr. hlasoví asistenti, softvér na analýzu fotografií, vyhľadávače, systémy rozpoznávania hlasu a tváre), ale umelá inteligencia môže byť aj súčasťou hardvérových zariadení (napr. vyspelé roboty, autonómne vozidlá, bezpilotné vzdušné prostriedky alebo aplikácie internetu vecí).“

[47] Expertná skupina na vysokej úrovni, definícia umelej inteligencie, s. 8: „Systémy umelej inteligencie sú softvérové (a prípadne aj hardvérové) systémy navrhnuté ľuďmi, ktoré vzhľadom na komplexnú úlohu konajú vo fyzickom alebo digitálnom rozmere tak, že vnímajú svoje prostredie prostredníctvom získavania údajov, interpretácie zhromaždených štruktúrovaných alebo neštruktúrovaných údajov, odvodzovania z poznatkov alebo spracúvania informácií odvodených z týchto údajov a že rozhodujú o najlepších krokoch, ktoré sa majú vykonať na dosiahnutie danej úlohy. Systémy umelej inteligencie môžu buď používať symbolické pravidlá, alebo sa naučiť numerický model, a takisto môžu upraviť svoje správanie na základe analýzy vplyvu, aký malo ich predchádzajúce konanie na prostredie.“

budú naďalej uplatňovať aj v súvislosti s umelou inteligenciou, hoci možno bude potrebné niektoré prvky tohto rámca aktualizovať, aby sa zohľadnila digitálna transformácia a využívanie umelej inteligencie (pozri oddiel B). Preto sa tie aspekty, ktorými sa už zaoberajú existujúce horizontálne alebo odvetvové právne predpisy (napr. o zdravotníckych pomôckach[48] či dopravných systémoch), budú naďalej riadiť týmito predpismi.

Nový regulačný rámec pre umelú inteligenciu by mal byť v zásade účinný na dosiahnutie cieľov, ktoré bude sledovať, ale zároveň by nemal byť príliš normatívny, aby nevytváral neprimeranú záťaž, najmä pre MSP. V záujme tejto rovnováhy sa Komisia domnieva, že by sa mala riadiť prístupom založeným na riziku.

Prístup založený na riziku je dôležitý na to, aby sa zabezpečilo, že regulačné zásahy budú primerané. Vyžaduje si však jasné kritériá rozlišovania medzi rôznymi aplikáciami umelej inteligencie, najmä pokiaľ ide o otázku, či sú alebo nie sú „vysokorizikové“[49]. Rozhodovanie o tom, či je určitá aplikácia umelej inteligencie vysokoriziková alebo nie, by malo byť jasné, ľahko pochopiteľné a uplatniteľné pre všetky dotknuté strany. Hoci nejaká aplikácia umelej inteligencie nemusí byť kvalifikovaná ako vysokoriziková, aj tak sa na ňu v plnej miere vzťahujú už existujúce pravidlá EÚ.

Komisia sa domnieva, že určitá aplikácia umelej inteligencie by sa mala vo všeobecnosti považovať za vysokorizikovú vzhľadom na to, aké sú hrozby, a či tak odvetvie, ako aj zamýšľané použitie zahŕňajú významné riziká, najmä z hľadiska ochrany bezpečnosti, práv spotrebiteľov a základných práv. Aplikácia umelej inteligencie by sa konkrétnejšie mala považovať za vysokorizikovú, ak spĺňa tieto dve kumulatívne kritériá:

- Po prvé, aplikácia umelej inteligencie sa používa v odvetví, kde vzhľadom na typické črty zvyčajne vykonávaných činností možno očakávať vznik významných rizík. Týmto prvým kritériom sa zabezpečuje, že regulačná intervencia sa bude sústreďovať na oblasti, v ktorých je pravdepodobnosť rizík vo všeobecnosti najvyššia. Dotknuté odvetvia by mali byť v novom regulačnom rámci konkrétne a podrobne vymenované. Napríklad zdravotná starostlivosť, doprava, energetika a časti verejného sektora[50]. Zoznam by sa mal pravidelne revidovať a v prípade potreby meniť v závislosti od príslušného vývoja v praxi.
- Po druhé, aplikácia umelej inteligencie v predmetnom odvetví sa okrem toho používa takým spôsobom, že existuje pravdepodobnosť vzniku značných rizík. Toto druhé kritérium odráža skutočnosť, že nie každé použitie umelej inteligencie vo vybraných sektoroch nevyhnutne zahŕňa značné riziká. Napríklad, zatiaľ čo zdravotná starostlivosť môže byť vo všeobecnosti relevantným odvetvím, chyba v rezervačnom systéme pre pacientov nemocníc zvyčajne nepredstavuje riziko takého významu, že by si vyžadovalo legislatívnu intervenciu. Posúdenie úrovne rizika daného použitia by mohlo vychádzať z vplyvu na dotknuté strany. Napríklad používanie aplikácií umelej inteligencie, ktoré má právne alebo podobne významné účinky na práva jednotlivca alebo spoločnosti, pri ktorom hrozí riziko poranenia, smrti alebo významnej

[48] Existujú rozličné bezpečnostné aspekty a právne dôsledky spojené napríklad so systémami umelej inteligencie, ktoré lekárom poskytujú špecializované lekárske informácie, systémami umelej inteligencie, ktoré poskytujú lekárske informácie priamo pacientovi, a systémami umelej inteligencie, ktoré samy vykonávajú zdravotnícke úkony priamo na pacientovi. Komisia skúma tieto problémy spojené s bezpečnosťou a so zodpovednosťou, ktoré sú špecifické pre zdravotnú starostlivosť.

[49] Právne predpisy EÚ môžu kategorizovať „riziká“ odlišne od toho, čo sa tu opisuje. Závisí to od oblasti, ako je napríklad bezpečnosť výrobkov.

[50] Verejný sektor by mohol zahŕňať oblasti ako azyl, migrácia, hraničné kontroly a súdnictvo, sociálne zabezpečenie či služby zamestnanosti.

materiálnej alebo nemateriálnej škody, prípadne ktoré má účinky, ktorým jednotlivci alebo právnické osoby nemôžu zabrániť.

Uplatňovaním týchto dvoch kumulatívnych kritérií by sa zabezpečilo, že rozsah pôsobnosti regulačného rámca by bol cielený a poskytoval by právnu istotu. Povinné požiadavky obsiahnuté v novom regulačnom rámci pre umelú inteligenciu (pozri oddiel D) by sa v zásade uplatňovali len na tie aplikácie, ktoré boli identifikované ako vysokorizikové v súlade s týmito dvoma kumulatívnymi kritériami.

Bez ohľadu na uvedené skutočnosti sa môžu vyskytnúť výnimočné prípady, keď by sa vzhľadom na riziká, o ktoré ide, používanie aplikácií umelej inteligencie na určité účely malo považovať za vysokorizikové – t. j. bez ohľadu na príslušný sektor. V takýchto prípadoch by sa uplatňovali požiadavky uvedené nižšie[51]. Na ilustráciu možno uviesť takýto príklad:

- Používanie aplikácií umelej inteligencie na prijímanie zamestnancov, ako aj v situáciách ovplyvňujúcich práva pracovníkov by sa vzhľadom na jeho význam pre jednotlivcov a so zreteľom na *acquis* EÚ, ktoré sa týka otázky rovnakého zaobchádzania v zamestnaní, vždy považovalo za vysokorizikové, a preto by sa naň mali vždy uplatňovať požiadavky uvedené nižšie. Mohli by sa posúdiť aj ďalšie špecifické aplikácie, ktoré by mohli mať vplyv na práva spotrebiteľov.

- Používanie aplikácií umelej inteligencie na účely diaľkovej biometrickej identifikácie[52] a iných invazívnych sledovacích technológií by sa vždy považovalo za vysokorizikové, a preto by sa naň vždy mali uplatňovať požiadavky uvedené nižšie.

D. DRUHY POŽIADAVIEK

Pri navrhovaní budúceho regulačného rámca pre umelú inteligenciu bude potrebné rozhodnúť o druhoch záväzných právnych požiadaviek, ktoré bude treba uložiť príslušným subjektom. Tieto požiadavky možno ďalej špecifikovať v normách. Ako sa uvádza v oddiele C, tieto požiadavky by sa okrem už existujúcich právnych predpisov uplatňovali len na vysokorizikové aplikácie umelej inteligencie, čím by sa zabezpečilo správne zameranie a primeranosť všetkých regulačných zásahov.

Vzhľadom na usmernenia expertnej skupiny na vysokej úrovni a so zreteľom na uvedené skutočnosti by požiadavky na vysokorizikové aplikácie umelej inteligencie mohli pozostávať z týchto kľúčových prvkov, ktoré sa podrobnejšie načrtávajú v nasledujúcich pododdieloch:

- údaje o výcviku,
- uchovávanie údajov a vedenie záznamov,
- informácie, ktoré sa majú poskytnúť,
- spoľahlivosť a presnosť,
- ľudský dohľad,

[51] Treba zdôrazniť, že sa môžu uplatňovať aj iné právne predpisy EÚ. Napríklad ak sú aplikácie umelej inteligencie súčasťou spotrebného tovaru, môže sa na ich bezpečnosť vzťahovať smernica o všeobecnej bezpečnosti výrobkov.

[52] Diaľková biometrická identifikácia by sa mala odlíšiť od biometrického overovania (čo je proces bezpečnostnej ochrany, ktorý sa opiera o jedinečné biologické vlastnosti jednotlivca, aby sa overila jeho deklarovaná totožnosť). Diaľková biometrická identifikácia spočíva v tom, že za pomoci biometrických identifikátorov (odtlačky prstov, podoba tváre, dúhovka, mapa žíl atď.) sa nepretržitým alebo priebežným overovaním údajov uložených v určitej databáze na diaľku stanovuje totožnosť viacerých osôb, a to na verejnom priestranstve.

- osobitné požiadavky na určité konkrétne aplikácie umelej inteligencie, napríklad tie, ktoré sa používajú na diaľkovú biometrickú identifikáciu.

V záujme právnej istoty sa tieto požiadavky bližšie určia s cieľom poskytnúť jasný štandard pre všetkých aktérov, ktorí ich musia dodržiavať.

a) Údaje použité na výcvik

Nikdy nebolo také dôležité podporovať, posilňovať a obhajovať hodnoty a pravidlá EÚ, a najmä práva, ktoré občanom vyplývajú z právnych predpisov EÚ. Toto úsilie sa nepochybne týka aj vysokorizikových aplikácií umelej inteligencie, ktoré sa uvádzajú na trh a používajú v EÚ a ktorých sa týka tento dokument.

Ako už bolo uvedené, umelá inteligencia nemôže existovať bez údajov. Fungovanie mnohých systémov umelej inteligencie a opatrenia a rozhodnutia, ku ktorým môžu viesť, vo veľkej miere závisia od dátových súborov, na ktorom boli systémy vycvičené. Preto by sa mali prijať potrebné opatrenia, aby sa v prípade údajov používaných na výcvik systémov umelej inteligencie, dodržiavali hodnoty a pravidlá EÚ, najmä pokiaľ ide o bezpečnosť a existujúce právne predpisy na ochranu základných práv. Mohlo by sa uvažovať o stanovení týchto požiadaviek týkajúcich sa dátových súborov na výcvik systémov umelej inteligencie:

- požiadavky, ktorých cieľom je poskytnúť primeranú istotu o tom, že následné použitie produktov alebo služieb založených na systéme umelej inteligencie je bezpečné, pretože spĺňa normy stanovené v platných bezpečnostných pravidlách EÚ (existujúce aj prípadné doplňujúce pravidlá). Príkladom sú požiadavky na zaistenie toho, aby sa systémy umelej inteligencie cvičili na súboroch údajov, ktoré sú dostatočne rozsiahle a zahŕňajú všetky relevantné scenáre, aby sa predišlo nebezpečným situáciám,

- požiadavky na prijatie primeraných opatrení, aby takéto následné používanie systémov umelej inteligencie neviedlo k zakázaným formám diskriminácie. Tieto požiadavky by mohli zahŕňať najmä povinnosti používať dátové súbory, ktoré sú dostatočne reprezentatívne, najmä preto, aby sa v nich primerane zohľadnili všetky relevantné rozmery pohlavia, etnického pôvodu a iných možných dôvodov zakázanej diskriminácie,

- požiadavky zamerané na zabezpečenie primeranej ochrany súkromia a osobných údajov pri používaní produktov a služieb založených na umelej inteligencii. Tieto otázky upravuje aj všeobecné nariadenie o ochrane údajov a smernica o presadzovaní práva, a to v závislosti od rozsahu ich pôsobnosti.

b) Vedenie záznamov a uchovávanie údajov

Vzhľadom na také prvky, ako sú komplexnosť a nepriehľadnosť mnohých systémov umelej inteligencie a s tým súvisiace ťažkosti, ktoré môžu komplikovať účinné overovanie dodržiavania uplatniteľných pravidiel a ich presadzovanie, sú potrebné požiadavky týkajúce sa vedenia záznamov v súvislosti s programovaním algoritmov a s údajmi používanými na výcvik vysokorizikových systémov umelej inteligencie a v určitých prípadoch aj uchovávania samotných údajov. Tieto požiadavky v podstate umožňujú vysledovanie a overenie potenciálne problematických krokov alebo rozhodnutí prijatých systémami umelej inteligencie. To by malo jednak uľahčiť dohľad a presadzovanie a jednak zvýšiť stimuly pre dotknuté hospodárske subjekty, aby zohľadňovali tieto pravidlá vo včasnom štádiu.

Na tento účel by regulačný rámec mohol stanovovať, aby sa uchovávali tieto prvky:

- presné záznamy týkajúce sa dátového súboru používaného na výcvik a testovanie systémov umelej inteligencie vrátane opisu hlavných charakteristík a spôsobu výberu súboru údajov,

- v určitých odôvodnených prípadoch samotné dátové súbory,

- dokumentácia o metódach programovania[53] a výcviku, postupoch a technikách použitých na výstavbu, testovanie a validáciu systémov umelej inteligencie, prípadne vrátane informácií o bezpečnosti a o tom, ako sa zabránilo zaujatosti, ktorá by mohla viesť k zakázaným formám diskriminácie.

Záznamy, dokumentácia a prípadne aj dátové súbory by sa mali uchovávať počas obmedzeného primeraného obdobia, aby sa zabezpečilo účinné presadzovanie príslušných právnych predpisov. Mali by sa prijať opatrenia na zabezpečenie ich dostupnosti na požiadanie, najmä na účely skúšania alebo kontroly príslušnými orgánmi. V prípade potreby by sa mali prijať opatrenia na zaistenie ochrany dôverných informácií, ako sú obchodné tajomstvá.

c) Poskytovanie informácií

Transparentnosť je potrebná aj nad rámec požiadaviek na vedenie záznamov, o ktorých sa hovorí v písmene c). Na dosiahnutie sledovaných cieľov, najmä pokiaľ ide o podporu zodpovedného využívania umelej inteligencie, budovanie dôvery a uľahčenie nápravy tam, kde je to potrebné, je dôležité, aby sa proaktívne poskytovali vhodné informácie o využívaní vysokorizikových systémov umelej inteligencie.

Preto by sa mohlo zvážiť stanovenie týchto požiadaviek:

- zabezpečenie jasných informácií, ktoré sa majú poskytnúť v súvislosti s kapacitami a obmedzeniami systému umelej inteligencie, najmä pokiaľ ide o účel, na ktorý sú systémy určené, podmienky, za ktorých možno očakávať, že spĺňajú plánovaný účel, a očakávanú úroveň presnosti pri dosahovaní konkrétneho účelu. Tieto informácie sú dôležité najmä pre používateľov systémov, ale môžu byť relevantné aj pre príslušné orgány a dotknuté strany.

- Navyše by občania mali byť jasne informovaní, keď sú v kontakte so systémom umelej inteligencie, a nie s človekom. Zatiaľ čo právne predpisy EÚ o ochrane údajov už obsahujú určité pravidlá tohto druhu[54], na dosiahnutie uvedených cieľov možno budú potrebné dodatočné požiadavky. V tom prípade by sa malo zabrániť zbytočnému zaťaženiu. Preto by sa takéto informácie nemuseli poskytovať napríklad v situáciách, keď je občanom okamžite zrejmé, že komunikujú so systémom umelej inteligencie. Okrem toho je dôležité, aby poskytnuté informácie boli objektívne, stručné a ľahko zrozumiteľné. Spôsob poskytovania informácií by sa mal prispôsobiť konkrétnemu kontextu.

d) Spoľahlivosť a presnosť

Systémy umelej inteligencie – a tobôž vysokorizikové aplikácie umelej inteligencie – musia byť technicky spoľahlivé a presné, aby mohli byť dôveryhodné. Takéto systémy sa teda musia vyvíjať zodpovedne a s náležitým anticipačným zohľadnením možných rizík. Pri vývoji a fungovaní systémov

[53] Napríklad dokumentácia o algoritme vrátane toho, akú optimalizáciu model sleduje, aké váhy sú navrhnuté pre určité parametre vo východiskovom bode atď.

[54] Konkrétne podľa článku 13 ods. 2 písm. f) všeobecného nariadenia o ochrane údajov musia prevádzkovatelia v čase získania osobných údajov poskytnúť dotknutým osobám ďalšie informácie o existencii automatizovaného rozhodovania a o určité dodatočné informácie, aby sa zabezpečilo spravodlivé a transparentné spracúvanie.

umelej inteligencie sa musí zabezpečiť, aby sa správali tak spoľahlivo, ako sa pôvodne plánovalo. Mali by sa prijať všetky primerané opatrenia na minimalizáciu rizika škody.

Preto by sa mali zvážiť tieto prvky:

- požiadavky, ktorými sa zabezpečí, aby boli systémy umelej inteligencie spoľahlivé a presné alebo aspoň správne odrážali úroveň svojej presnosti počas všetkých fáz životného cyklu,

- požiadavky, ktorými sa zabezpečí reprodukovateľnosť výsledkov,

- požiadavky, ktorými sa zabezpečí, aby systémy umelej inteligencie mohli primerane riešiť chyby alebo nezrovnalosti počas všetkých fáz životného cyklu,

- požiadavky, ktorými sa zabezpečí, aby boli systémy umelej inteligencie odolné voči zjavným útokom a jemnejším pokusom o manipuláciu s údajmi alebo algoritmami, a aby sa v takýchto prípadoch prijali zmierňujúce opatrenia.

e) Ľudský dohľad

Ľudský dohľad pomáha garantovať, aby systém umelej inteligencie neoslaboval ľudskú autonómiu ani nespôsoboval iné nepriaznivé účinky. Cieľ dôveryhodnej a etickej umelej inteligencie sústredenej na človeka možno dosiahnuť len tak, že sa zaistí primerané zapojenie ľudí vo vzťahu k vysokorizikovým aplikáciám umelej inteligencie.

Aj keď sa všetky aplikácie umelej inteligencie, ktorými sa zaoberá táto biela kniha s ohľadom na konkrétny právny režim, považujú za vysokorizikové, primeraný druh a stupeň ľudského dohľadu sa môžu v jednotlivých prípadoch líšiť. Závisieť to bude najmä od zamýšľaného používania systémov a od účinkov, ktoré by používanie mohlo mať pre dotknutých občanov a právne subjekty. Zároveň tým nie sú dotknuté zákonné práva stanovené vo všeobecnom nariadení o ochrane údajov v situáciách, keď systém umelej inteligencie spracúva osobné údaje. Ľudský dohľad by mohol mať napríklad tieto podoby (ale nie výlučne):

- výstup systému umelej inteligencie sa nepoužije, pokiaľ ho predtým nepreskúma a neoverí človek (napr. zamietnuť žiadosť o dávky sociálneho zabezpečenia môže len človek),

- výstup systému umelej inteligencie sa okamžite použije, ale ľudský dohľad sa zabezpečí následne (napr. zamietnutie žiadosti o kreditnú kartu môže spracovať systém umelej inteligencie, ale človek musí mať možnosť ho neskôr skontrolovať),

- systém umelej inteligencie sa monitoruje počas prevádzky a dá sa doň zasiahnuť v reálnom čase a deaktivovať ho (napr. tlačidlo stop alebo možnosť v autonómnom vozidle, aby sa človek mohol rozhodnúť, že prevádzka nie je bezpečná),

- vo fáze návrhu sa zavedú prevádzkové obmedzenia systému umelej inteligencie (napríklad samojazdiace vozidlo zastaví prevádzku za určitých podmienok nízkej viditeľnosti, keď snímače môžu byť menej spoľahlivé, alebo v danej situácii udržiava určitú vzdialenosť od vozidla pred ním).

f) Osobitné požiadavky na diaľkovú biometrickú identifikáciu

Zber a používanie biometrických údajov [55] na diaľkovú identifikáciu [56], napríklad pomocou rozpoznávania tváre na verejných miestach, prináša osobitné riziká z hľadiska základných práv[57]. Dôsledky používania systémov umelej inteligencie na diaľkovú biometrickú identifikáciu sa môžu značne líšiť v závislosti od účelu, kontextu a rozsahu použitia.

Pravidlá EÚ na ochranu údajov v zásade zakazujú spracúvanie biometrických údajov na účely jedinečnej identifikácie fyzickej osoby, pokiaľ sa neuplatňujú osobitné podmienky[58]. Konkrétne sa podľa všeobecného nariadenia o ochrane údajov k takémuto spracovaniu smie pristúpiť len z obmedzeného počtu dôvodov, pričom hlavný dôvod je závažný verejný záujem. V takom prípade spracúvanie musí prebiehať v súlade s právom EÚ alebo vnútroštátnym právom, a to s výhradou požiadaviek proporcionality, dodržiavania podstaty práva na ochranu údajov a primeraných záruk. Podľa smernice o presadzovaní práva musí byť takéto spracúvanie striktne nevyhnutné; v zásade naň treba povolenie podľa únijného alebo vnútroštátneho práva a musia sa uplatňovať primerané záruky. Keďže akékoľvek spracúvanie biometrických údajov na účely individuálnej identifikácie fyzickej osoby by sa týkalo výnimky zo zákazu stanoveného v práve EÚ, bolo by predmetom Charty základných práv EÚ.

Z toho vyplýva, že v súlade s platnými pravidlami EÚ v oblasti ochrany údajov a Chartou základných práv sa umelá inteligencia môže používať na diaľkovú biometrickú identifikáciu len vtedy, ak je takéto použitie riadne odôvodnené a primerané a ak podlieha primeraným zárukám.

S cieľom riešiť prípadné obavy spoločnosti týkajúce sa používania umelej inteligencie na takéto účely na verejných miestach a zabrániť fragmentácii vnútorného trhu Komisia začne rozsiahlu európsku diskusiu o prípadných osobitných okolnostiach, ktoré by mohli takéto použitie odôvodniť, a o spoločných zárukách.

E. ADRESÁTI

Pokiaľ ide o adresátov právnych požiadaviek, ktoré by sa uplatňovali v súvislosti s uvedenými vysokorizikovými aplikáciami umelej inteligencie, treba zvážiť dva hlavné problémy.

Prvá otázka je, ako sa majú povinnosti rozdeliť medzi zúčastnené hospodárske subjekty. Do životného cyklu systému umelej inteligencie sú zapojené mnohé subjekty. K nim patria vývojári, prevádzkovatelia (osoby, ktoré používajú produkt alebo službu s prvkami umelej inteligencie)

---

[55] Biometrické údaje sa vymedzujú ako „osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako sú vyobrazenia tváre alebo daktyloskopické údaje [údaje o odtlačkoch prstov]“; [článok 3 ods. 13 smernice o presadzovaní práva; článok 4 ods. 14 všeobecného nariadenia o ochrane údajov; článok 3 ods. 18 nariadenia (EÚ) 2018/1725].

[56] Pokiaľ ide o rozpoznávanie tváre, identifikácia znamená, že vzor podoby tváre určitej osoby sa porovná s mnohými inými vzormi uloženými v databáze s cieľom zistiť, či sa v nej nachádza podoba tváre tejto osoby. Overovanie (autentifikácia) sa na druhej strane často označuje ako párovanie. Umožňuje porovnanie dvoch biometrických vzorov, ktoré zvyčajne patria tej istej fyzickej osobe. Dva biometrické vzory sa porovnávajú, aby sa určilo, či osoba zobrazená na dvoch snímkach je tou istou osobou. Takýto postup sa používa napríklad pri automatizovanej hraničnej kontrole, ktorá sa používa na hraničné kontroly na letiskách.

[57] Napríklad pokiaľ ide o ľudskú dôstojnosť. V tejto súvislosti sú ústredným aspektom základných práv pri používaní technológie rozpoznávania tváre práva na rešpektovanie súkromného života a ochranu osobných údajov. Netreba zabúdať ani na potenciálny vplyv na nediskrimináciu a práva osobitných skupín, ako sú deti, staršie osoby a osoby so zdravotným postihnutím. Využívanie technológie navyše nesmie ohroziť ani slobodu prejavu, združovania a zhromažďovania. Pozri: Technológia rozpoznávania tváre: problematika základných práv v kontexte presadzovania práva, https://fra.europa.eu/en/publication/2019/facial-recognition.

[58] Článok 9 všeobecného nariadenia o ochrane údajov, článok 10 smernice o presadzovaní práva. Pozri aj článok 10 nariadenia (EÚ) 2018/1725 (uplatňuje sa na inštitúcie a orgány EÚ).

a potenciálne ďalšie osoby (výrobca, distribútor alebo dovozca, poskytovateľ služieb, profesionálny alebo súkromný používateľ).

Komisia sa domnieva, že v budúcom regulačnom rámci by sa každá povinnosť mala prisúdiť účastníkom, ktorí dokážu najlepšie riešiť všetky potenciálne riziká. Napríklad vývojári umelej inteligencie síce sú možno najkompetentnejší, pokiaľ ide o riziká vyplývajúce z fázy vývoja, ale môže byť pre nich ťažšie kontrolovať riziká vo fáze používania. V takom prípade by mal podliehať príslušnej povinnosti prevádzkovateľ. Tým nie je dotknutá otázka, ktorá strana by mala byť zodpovedná za akúkoľvek spôsobenú škodu na účely zodpovednosti vo vzťahu ku konečným používateľom alebo k iným subjektom, ktoré utrpeli škodu a ktoré musia mať účinný prístup k spravodlivosti. Podľa právnych predpisov EÚ o zodpovednosti za výrobky sa zodpovednosť za chybné výrobky pripisuje výrobcovi bez toho, aby boli dotknuté vnútroštátne právne predpisy, ktoré môžu navyše umožniť vymáhanie od iných strán.

Druhá otázka sa týka geografického rozsahu legislatívneho zásahu. Podľa názoru Komisie je mimoriadne dôležité, aby sa požiadavky vzťahovali na všetky príslušné hospodárske subjekty poskytujúce produkty alebo služby s podporou umelej inteligencie v EÚ bez ohľadu na to, či v nej majú sídlo alebo nie. Inak by nebolo možné úplne dosiahnuť ciele legislatívnej intervencie uvedené vyššie.

F. SÚLAD A PRESADZOVANIE

Ak sa má zaručiť, aby bola umelá inteligencia dôveryhodná, bezpečná a v súlade s európskymi hodnotami a pravidlami, príslušné právne požiadavky sa musia dodržiavať aj v praxi a musia ich účinne presadzovať príslušné vnútroštátne a európske orgány, ako aj dotknuté strany. Príslušné orgány by mali dokázať vyšetrovať jednotlivé prípady, ale aj posúdiť vplyv na spoločnosť.

Vzhľadom na vysoké riziko, ktoré pre občanov a našu spoločnosť predstavujú určité aplikácie umelej inteligencie (pozri oddiel A), sa Komisia v tejto fáze domnieva, že by bolo treba najprv zrealizovať objektívne posúdenie zhody, aby mohla overiť a uistiť sa, či sú splnené niektoré z uvedených povinných požiadaviek uplatniteľných na vysokorizikové aplikácie (pozri oddiel D). Počiatočné posúdenie zhody by mohlo zahŕňať postupy skúšania, kontroly alebo certifikácie[59]. Jeho súčasťou by mohli byť kontroly algoritmov a dátových súborov používaných vo fáze vývoja.

Posudzovanie zhody pri vysokorizikových aplikáciách umelej inteligencie by malo byť súčasťou mechanizmov posudzovania zhody, ktoré už existujú v prípade množstva výrobkov uvádzaných na vnútorný trh EÚ. Ak sa nemožno spoľahnúť na žiadne takéto existujúce mechanizmy, možno bude potrebné vytvoriť podobné mechanizmy na základe najlepších postupov a prípadného príspevku zainteresovaných strán a európskych normalizačných organizácií. Každý takýto nový mechanizmus by mal byť primeraný a nediskriminačný a mal by používať transparentné a objektívne kritériá v súlade s medzinárodnými záväzkami.

Pri navrhovaní a zavádzaní systému, ktorý sa by opieral o počiatočné posúdenia zhody, by sa mali osobitne zohľadniť tieto otázky:

[59] Systém by bol založený na postupoch posudzovania zhody v EÚ – pozri rozhodnutie 768/2008/ES alebo nariadenie (EÚ) 2019/881 (akt o kybernetickej bezpečnosti), pričom by sa zohľadnili osobitosti umelej inteligencie. Pozri Modrú príručku na vykonávanie právnych predpisov EÚ týkajúcich sa výrobkov, 2014.

- Počiatočné posúdenie zhody nemusí byť vhodné na overenie všetkých uvedených požiadaviek. Takéto posúdenie vo všeobecnosti nie je vhodné napríklad v prípade požiadavky na informácie, ktoré sa majú poskytovať.

- Osobitne by sa mala zohľadniť možnosť, že určité systémy umelej inteligencie sa vyvíjajú a učia zo skúseností, čo si môže vyžadovať opakované posúdenia počas ich životného cyklu.

- Treba overovať údaje použité na účely výcviku a príslušné metodiky, postupy a techniky programovania a výcviku používané na vytvorenie, skúšanie a validáciu systémov umelej inteligencie.

- Ak z posúdenia zhody vyplynie, že systém umelej inteligencie nespĺňa požiadavky týkajúce sa napríklad údajov používaných na jeho výcvik, zistené nedostatky sa budú musieť odstrániť – napríklad „preškolením“ systému v EÚ tak, aby sa zabezpečilo splnenie všetkých uplatniteľných požiadaviek.

Posudzovanie zhody by bolo povinné pre všetky hospodárske subjekty, na ktoré sa vzťahujú dané požiadavky, a to bez ohľadu na to, kde sídlia[60]. S cieľom obmedziť zaťaženie MSP by sa mohla zaviesť určitá podporná štruktúra, a to aj prostredníctvom centier digitálnych inovácií. Okrem toho by dosiahnutie súladu mohli uľahčiť normy či špecializované online nástroje.

Akékoľvek počiatočné posudzovanie zhody by nemalo mať vplyv na monitorovanie dodržiavania predpisov a presadzovanie príslušnými vnútroštátnymi orgánmi *ex post*. To platí pre vysokorizikové aplikácie umelej inteligencie, ale aj pre iné aplikácie umelej inteligencie, na ktoré sa vzťahujú právne požiadavky, hoci vysokoriziková povaha predmetných aplikácií môže byť pre príslušné vnútroštátne orgány dôvodom, aby im venovali osobitnú pozornosť. Kontroly *ex post* by mali byť uľahčené tým, že bude k dispozícii primeraná dokumentácia príslušnej aplikácie umelej inteligencie (pozri oddiel E) a že tretie strany, ako sú napríklad príslušné orgány, budú mať v prípade potreby možnosť takéto aplikácie testovať. Môže to byť obzvlášť dôležité vtedy, keď dôjde k ohrozeniu základných práv v závislosti od kontextu. Takéto monitorovanie súladu by malo byť súčasťou systému priebežného dohľadu nad trhom. Aspekty týkajúce sa riadenia sú podrobnejšie opísané v oddiele H.

Okrem toho by sa mali zabezpečiť účinné súdne prostriedky nápravy pre strany, na ktoré majú systémy umelej inteligencie negatívny vplyv, a to tak v prípade vysokorizikových, ako aj iných aplikácií umelej inteligencie. Otázky týkajúce sa zodpovednosti sa ďalej rozoberajú v správe o rámci bezpečnosti a zodpovednosti sprevádzajúcej túto bielu knihu.

G. DOBROVOĽNÉ OZNAČOVANIE PRE APLIKÁCIE UMELEJ INTELIGENCIE, KTORÉ NIE SÚ VYSOKORIZIKOVÉ

Pokiaľ ide o aplikácie umelej inteligencie, ktoré sa nepovažujú za „vysokorizikové“ (pozri oddiel C), a na ktoré sa preto nevzťahujú povinné požiadavky uvedené vyššie (pozri oddiely D, E a F), jednou možnosťou by bolo popri uplatniteľných právnych predpisoch zaviesť aj systém dobrovoľného označovania.

V rámci tohto systému by sa zainteresované hospodárske subjekty, na ktoré sa nevzťahujú povinné požiadavky, mohli dobrovoľne rozhodnúť, že budú podliehať buď týmto požiadavkám, alebo určitému

[60] Pokiaľ ide o príslušnú riadiacu štruktúru vrátane orgánov určených na vykonávanie posudzovania zhody, pozri oddiel H.

súboru podobných požiadaviek, ktoré boli stanovené najmä na účely takéhoto dobrovoľného systému. Aplikáciám umelej inteligencie príslušných hospodárskych subjektov by potom bola udelená značka kvality.

Dobrovoľné označenie by umožnilo dotknutým hospodárskym subjektom signalizovať, že ich produkty a služby s podporou umelej inteligencie sú dôveryhodné. Umožnilo by používateľom ľahko rozpoznať, že príslušné výrobky a služby sú v súlade s určitými objektívnymi a štandardizovanými únijnými kritériami, ktoré prekračujú rámec bežných platných právnych povinností. Pomohlo by to zvýšiť dôveru používateľov v systémy umelej inteligencie a podporiť celkové využívanie tejto technológie.

Táto možnosť by si vyžadovala vytvorenie nového právneho nástroja, ktorý by stanovil dobrovoľný rámec označovania pre vývojárov a/alebo prevádzkovateľov systémov umelej inteligencie, ktoré sa nepovažujú za vysokorizikové. Hoci účasť na systéme označovania by bola dobrovoľná, ak by sa vývojár alebo prevádzkovateľ rozhodli toto označenie používať, požiadavky by sa stali záväznými. Plnenie všetkých požiadaviek by sa zabezpečovalo kombináciou presadzovania *ex ante* a *ex post*.

H. RIADENIE

V záujme toho, aby sa zabránilo roztrieštenosti zodpovednosti, aby sa zvýšila kapacita členských štátov a aby sa Európa postupne vybavila kapacitou potrebnou na skúšanie a certifikáciu produktov a služieb s podporou umelej inteligencie, je potrebná európska riadiaca štruktúra v oblasti umelej inteligencie, ktorá by mala podobu rámca spolupráce príslušných vnútroštátnych orgánov. V tejto súvislosti by bolo prospešné podporiť príslušné vnútroštátne orgány, aby mohli plniť svoj mandát v situáciách, v ktorých sa používa umelá inteligencia.

Európska riadiaca štruktúra by mohla mať rôzne úlohy – mohla by predstavovať fórum na pravidelnú výmenu informácií a najlepších postupov, identifikáciu nových trendov či poskytovanie poradenstva o normalizačnej činnosti a certifikácii. Mala by tiež zohrávať kľúčovú úlohu pri uľahčovaní vykonávania právneho rámca, a to napríklad tak, že by vydávala usmernenia, stanoviská a poskytovala odborné poradenstvo. Na tento účel by sa mala opierať o sieť vnútroštátnych orgánov, ako aj sektorových sietí a regulačných orgánov na vnútroštátnej aj únijnej úrovni. Okrem toho by mohol existovať výbor odborníkov, ktorý by poskytoval pomoc Komisii.

Riadiaca štruktúra by mala zaručovať maximálnu účasť zainteresovaných strán. O vykonávaní a ďalšom rozvoji rámca by sa malo konzultovať so zainteresovanými stranami – spotrebiteľskými organizáciami a sociálnymi partnermi, podnikmi, výskumnými pracovníkmi a organizáciami občianskej spoločnosti.

Vzhľadom na existujúce štruktúry v oblastiach, ako sú financie, lieky, letectvo, zdravotnícke pomôcky, ochrana spotrebiteľa či ochrana údajov, by navrhovaná štruktúra riadenia nemala duplikovať existujúce funkcie. Namiesto toho by mala nadviazať úzke väzby s inými orgánmi EÚ a príslušnými vnútroštátnymi orgánmi v rôznych odvetviach s cieľom doplniť existujúce odborné znalosti a pomôcť existujúcim orgánom pri monitorovaní a dohľade nad činnosťami hospodárskych subjektov, ktorých súčasťou sú systémy umelej inteligencie a produkty a služby s podporou umelej inteligencie.

Napokon treba dodať, že ak sa táto možnosť uskutoční, vykonávaním posudzovania zhody by sa mohli poveriť notifikované osoby určené členskými štátmi. Nezávislý audit a hodnotenie systémov umelej inteligencie v súlade s požiadavkami uvedenými vyššie by mali umožniť skúšobné strediská. Nezávislým hodnotením sa zvýši dôvera a zabezpečí sa objektívnosť. Mohlo by to takisto uľahčiť prácu dotknutým príslušným orgánom.

EÚ disponuje excelentnými skúšobnými a hodnotiacimi strediskami a mala by rozvíjať svoje kapacity aj v oblasti umelej inteligencie. Hospodárske subjekty so sídlom v tretích krajinách, ktoré chcú vstúpiť na vnútorný trh, by mohli buď využiť určené orgány so sídlom v EÚ, alebo – s výhradou dohôd o vzájomnom uznávaní s tretími krajinami – využiť orgány tretích krajín určené na vykonanie takéhoto posúdenia.

Riadiaca štruktúra v súvislosti s umelou inteligenciou a možné posudzovanie zhody, ktoré sa tu spomínajú, by nemali nijaký vplyv na právomoci a zodpovednosti relevantných príslušných orgánov v konkrétnych sektoroch alebo v špecifických otázkach (financie, lieky, letectvo, zdravotnícke pomôcky, ochrana spotrebiteľa, ochrana údajov atď.), ktoré vyplývajú z existujúcich právnych predpisov EÚ.

6. ZÁVER

Umelá inteligencia je strategická technológia, ktorá ponúka mnoho výhod občanom, podnikom a spoločnosti ako celku – za predpokladu, že je sústredená na človeka, etická, udržateľná a že dodržiava základné práva a hodnoty. Umelá inteligencia ponúka významné zvýšenie efektívnosti a produktivity, ktoré môže posilniť konkurencieschopnosť európskeho priemyslu a zlepšiť životné podmienky obyvateľstva. Môže tiež prispieť k riešeniu niektorých najnaliehavejších spoločenských problémov vrátane boja proti zmene klímy a zhoršovaniu životného prostredia, výziev spojených s udržateľnosťou, demografickými zmenami a ochranou našich demokracií a (v prípade potreby a v primeraných medziach) aj v boji proti trestnej činnosti.

Aby Európa mohla v plnej miere využiť príležitosti, ktoré ponúka umelá inteligencia, musí budovať a posilňovať potrebné priemyselné a technologické kapacity. Ako sa uvádza v sprievodnej európskej dátovej stratégii, to si vyžaduje aj opatrenia, ktoré umožnia EÚ stať sa globálnym centrom pre dáta.

Cieľom európskeho prístupu k umelej inteligencii je podporovať inovačnú kapacitu Európy v oblasti umelej inteligencie a zároveň podporovať rozvoj a zavádzanie etickej a dôveryhodnej umelej inteligencie v celom hospodárstve EÚ. Umelá inteligencia by mala slúžiť ľuďom a byť hybnou silou pre dobro v spoločnosti.

Komisia zverejnením tejto bielej knihy a sprievodnej správy o rámci bezpečnosti a zodpovednosti otvára rozsiahle konzultácie s občianskou spoločnosťou, priemyslom a akademickou obcou členských štátov o konkrétnych návrhoch európskeho prístupu k umelej inteligencii. Patria sem politické prostriedky na zvýšenie investícií do výskumu a inovácií, zlepšenie rozvoja zručností a podpory zavádzania umelej inteligencie zo strany MSP, ako aj návrhy kľúčových prvkov budúceho regulačného rámca. Táto konzultácia umožní komplexný dialóg so všetkými zainteresovanými stranami, z ktorého budú vychádzať ďalšie kroky Komisie.

Komisia vyzýva na predloženie pripomienok k návrhom uvedeným v bielej knihe prostredníctvom otvorenej verejnej konzultácie, ktorá je k dispozícii na adrese https://ec.europa.eu/info/consultations_sk. Konzultácia je otvorená do 19. mája 2020.

Bežnou praxou Komisie je uverejňovať príspevky prijaté v rámci verejných konzultácií. Je však možné požiadať, aby príspevky alebo ich časti neboli uverejnené. V takom prípade je potrebné zreteľne uviesť na prvej strane uvedeného dokumentu, že nemá byť uverejnený, a okrem toho poslať verziu dokumentu, ktorá nie je dôverná, Komisii na uverejnenie.