EVROPSKA
KOMISIJA

Bruselj, 19.2.2020
COM(2020) 65 final

BELA KNJIGA

o umetni inteligenci - evropski pristop k odličnosti in zaupanju

Bela knjiga o umetni inteligenci
Evropski pristop k odličnosti in zaupanju

Umetna inteligenca se hitro razvija in bo spremenila naša življenja z izboljšanjem zdravstvenega varstva (na primer z natančnejšimi diagnostikami in boljšim preprečevanjem bolezni), povečanjem učinkovitosti kmetijstva, prispevanjem k blaženju podnebnih sprememb in prilagajanju nanje, povečanjem učinkovitosti proizvodnih sistemov z napovednim vzdrževanjem, izboljšanjem varnosti Evropejcev in Evropejk in še na številne druge načine, ki si jih ne moremo še niti zamisliti. Obenem prinaša tudi vrsto možnih tveganj, kot so nepregledno odločanje, diskriminacija na podlagi spola ali druge oblike diskriminacije, vdor v zasebno življenje ali njena uporaba za kazniva dejanja.

Zaradi močne svetovne konkurence potrebujemo trden evropski pristop, ki temelji na evropski strategiji za umetno inteligenco, predstavljeni aprila 2018[1]. Da bi EU lahko obravnavala priložnosti in izzive umetne inteligence, mora ukrepati enotno ter opredeliti svojo pot k spodbujanju njenega razvoja in uvajanja na podlagi evropskih vrednot.

Komisija je odločena, da bo omogočila znanstveni prodor, ohranila vodilno vlogo EU na področju tehnologije in zagotovila, da bodo nove tehnologije služile vsem Evropejcem in Evropejkam, tako da bodo izboljšale njihova življenja ter hkrati spoštovale njihove pravice.

Predsednica Komisije Ursula von der Leyen je v svojih političnih usmeritvah[2] napovedala usklajen evropski pristop k družbenim in etičnim posledicam umetne inteligence ter razmislek o boljši uporabi velepodatkov za inovacije.

Komisija zato podpira regulativen in v naložbe usmerjen pristop z dvojnim ciljem – širjenje uporabe umetne inteligence in obravnavanje tveganj, povezanih z nekaterimi vrstami uporabe te nove tehnologije. Namen te bele knjige je določiti politične možnosti za dosego teh ciljev. Bela knjiga ne obravnava razvoja in uporabe umetne inteligence za vojaške namene. Komisija poziva države članice, druge evropske institucije in vse zainteresirane strani, vključno z industrijo, socialnimi partnerji, organizacijami civilne družbe, raziskovalci, širšo javnostjo in vsemi drugimi deležniki, naj izrazijo svoje mnenje o navedenih možnostih in tako prispevajo k prihodnjim odločitvam Komisije na tem področju.

1. UVOD

Ker je digitalna tehnologija vedno bolj osrednji del vsakega vidika življenja, je pomembno, da ji ljudje lahko zaupajo. Zaupanje je tudi pogoj za njeno uporabo. To je priložnost za Evropo, ki daje velik pomen vrednotam in pravni državi ter je dokazano sposobna razviti varne, zanesljive in napredne proizvode ter storitve v različnih sektorjih, od aeronavtike do energetike, avtomobilske industrije in sektorja medicinske opreme.

Sedanja in prihodnja trajnostna gospodarska rast in družbena blaginja v Evropi se vedno bolj opirata na vrednost, ki jo ustvarjajo podatki. Umetna inteligenca je ena od najpomembnejših aplikacij podatkovnega gospodarstva. Danes je večina podatkov povezanih s potrošniki in se obdelujejo v osrednji infrastrukturi v oblaku. Po drugi strani bo v prihodnje velik delež vse večjega števila podatkov izhajal iz industrije, gospodarstva in javnega sektorja, podatki pa bodo shranjeni v različnih

[1] Umetna inteligenca za Evropo (COM(2018) 237 final).
[2] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_sl.pdf.

sistemih, zlasti v računalniških napravah, ki delujejo na robu omrežja. To odpira nove priložnosti za Evropo, ki ima močen položaj v digitalizirani industriji in pri aplikacijah „podjetje-podjetje“, toda razmeroma šibek položaj na področju potrošniških platform.

Preprosto povedano, umetna inteligenca je zbirka tehnologij, ki združuje podatke, algoritme in računalniške zmogljivosti. Napredek na področju računalništva in vedno večja razpoložljivost podatkov sta torej ključna dejavnika sedanjega porasta umetne inteligence. Evropa lahko svoje tehnološke in industrijske prednosti združi z visokokakovostno digitalno infrastrukturo in regulativnim okvirom, osnovanim na njenih temeljnih vrednotah, in **postane vodilna v svetu pri inovacijah na področju podatkovnega gospodarstva in njegovih aplikacij**, kot je določeno v evropski podatkovni strategiji[3]. Na tej podlagi lahko razvije umetnointeligenčni ekosistem, ki bo koristi tehnologije prinašal vsej evropski družbi in gospodarstvu:

- **državljanke in državljani** bodo lahko koristili nove prednosti, kot so boljše zdravstveno varstvo, manjše število okvar gospodinjskih naprav, varnejši in čistejši prometni sistemi ter boljše javne storitve,
- **podjetja** bodo na primer lahko razvijala novo generacijo proizvodov in storitev na področjih, na katerih je Evropa še posebej uspešna (stroji, prevoz, kibernetska varnost, kmetijstvo, zeleno in krožno gospodarstvo, zdravstvo in sektorji z visoko dodano vrednostjo, kot sta sektorja mode in turizma),
- pri storitvah **javnega interesa** (promet, izobraževanje, energija in ravnanje z odpadki) pa se bodo lahko na primer zmanjšali stroški njihovega zagotavljanja, izboljšala trajnostnost proizvodov [4] in zagotovila ustrezna orodja organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, da bodo lahko zaščitili državljanke in državljane[5], ob ustreznih zaščitnih ukrepih za spoštovanje njihovih pravic in svoboščin.

Glede na velik vpliv umetne inteligence na našo družbo in potrebo po vzpostavitvi zaupanja je nujno, da evropska umetna inteligenca temelji na naših vrednotah in temeljnih pravicah, kot sta človekovo dostojanstvo in varstvo zasebnosti.

Poleg tega se vpliv sistemov umetne inteligence ne bi smel obravnavati samo s stališča posameznika, temveč tudi s stališča družbe kot celote. Uporaba sistemov umetne inteligence ima lahko pomembno vlogo pri doseganju ciljev trajnostnega razvoja ter podpiranju demokratičnega procesa in socialnih pravic. Glede na nedavne predloge o evropskem zelenem dogovoru[6] je Evropa vodilna pri spopadanju s podnebnimi izzivi in izzivi, povezanimi z okoljem. Digitalne tehnologije, kot je umetna inteligenca, so pomemben dejavnik pri izpolnjevanju ciljev zelenega dogovora. Ker ima umetna inteligenca vse večji pomen, je treba ustrezno upoštevati vpliv sistemov umetne inteligence na okolje v njihovem celotnem življenjskem ciklu in vzdolž celotne dobavne verige, na primer kar zadeva uporabo virov za učenje algoritmov in shranjevanje podatkov.

[3] COM(2020) 66 final.

[4] Umetna inteligenca in digitalizacija na splošno sta ključna dejavnika, ki bosta omogočila doseganje ciljev evropskega zelenega dogovora. Vendar je trenutni okoljski odtis sektorja IKT ocenjen na več kot 2 % vseh svetovnih emisij. V evropski digitalni strategiji, ki je priložena tej beli knjigi, so predlagani ukrepi zelene preobrazbe za digitalno področje.

[5] Orodja umetne inteligence so lahko priložnost za boljšo zaščito državljank in državljanov EU pred kriminalom in terorističnimi dejanji.

Takšna orodja bi lahko na primer pomagala pri odkrivanju spletne teroristične propagande, sumljivih transakcij pri prodaji nevarnih proizvodov, nevarnih skritih predmetov ali prepovedanih snovi in proizvodov, pomagala državljankam in državljanom v izrednih razmerah ter podpirala usmerjanje služb, ki se prve odzovejo.

[6] COM(2019) 640 final.

Skupni evropski pristop k umetni inteligenci je potreben, da se doseže zadosten obseg in prepreči razdrobljenost enotnega trga. Z uvedbo nacionalnih pobud bi se lahko ogrozila pravna varnost, zmanjšalo zaupanje državljank in državljanov ter preprečil razvoj dinamične evropske industrije.

V tej beli knjigi so predstavljene možnosti politike, ki naj bi omogočile zaupanja vreden in varen razvoj umetne inteligence v Evropi ob polnem spoštovanju vrednot in pravic državljank in državljanov EU. Glavni gradniki te bele knjige so:

- okvir politike, ki določa ukrepe za uskladitev prizadevanj na evropski, nacionalni in regionalni ravni. Cilj okvira je s partnerstvom med zasebnim in javnim sektorjem zbrati sredstva za vzpostavitev **„ekosistema odličnosti“** vzdolž celotne vrednostne verige, začenši z raziskavami in inovacijami, ter ustvariti prave spodbude za hitrejše sprejemanje rešitev, ki temeljijo na umetni inteligenci, med drugim tudi v malih in srednjih podjetjih (MSP),
- ključni elementi prihodnjega regulativnega okvira za umetno inteligenco v Evropi, ki bodo ustvarili edinstven **„ekosistem zaupanja“**. Da bi bilo to mogoče, mora okvir zagotoviti spoštovanje pravil EU, vključno s pravili o varstvu temeljnih pravic in pravic potrošnikov, kar velja zlasti za sisteme umetne inteligence, ki delujejo v EU in predstavljajo veliko tveganje[7]. Vzpostavitev ekosistema zaupanja je že sama po sebi cilj politike, saj naj bi ta ekosistem državljankam in državljanom vlil zaupanje v uporabo umetne inteligence, podjetjem in javnim organizacijam pa zagotovil pravno varnost za inovacije z uporabo umetne inteligence. Komisija močno podpira humanocentričen pristop, ki temelji na sporočilu o krepitvi zaupanja v umetno inteligenco, osredotočeno na človeka[8], in bo upoštevala tudi prispevke, pridobljene v pilotni fazi priprave etičnih smernic strokovne skupine na visoki ravni za umetno inteligenco.

Namen evropske strategije za podatke, ki je priložena tej beli knjigi, je omogočiti Evropi, da postane najprivlačnejše, najvarnejše in najbolj dinamično podatkovno okretno gospodarstvo na svetu, kar bo Evropo opolnomočilo, da s podatki izboljša odločanje ter življenja vseh državljank in državljanov. Strategija določa številne ukrepe politike, vključno s pritegnitvijo zasebnih in javnih naložb, ki so potrebne za dosego tega cilja. V poročilu Komisije, ki je priloženo tej beli knjigi, so analizirane tudi posledice umetne inteligence, interneta stvari in drugih digitalnih tehnologij za zakonodajo o varnosti in odgovornosti.

2. IZKORIŠČANJE PREDNOSTI NA INDUSTRIJSKIH IN SPECIALIZIRANIH TRGIH

Evropa je v dobrem položaju, da izkoristi potencial umetne inteligence, in sicer ne le kot uporabnica, temveč tudi kot razvijalka in proizvajalka te tehnologije. Ima odlične raziskovalne centre, inovativna zagonska podjetja, vodilno vlogo v svetu na področju robotike ter konkurenčne proizvodne in storitvene sektorje, od avtomobilske industrije do zdravstvenega varstva, energetike, finančnih storitev in kmetijstva. Razvila je močno računalniško infrastrukturo (na primer visokozmogljivostne računalnike), ki je ključna za delovanje umetne inteligence. Prav tako ima velike količine javnih in industrijskih podatkov, katerih potencial se trenutno premalo izkorišča. Evropa ima tudi dobro priznane industrijske prednosti na področju varnih in zanesljivih digitalnih sistemov z nizko porabo, ki so bistvenega pomena za nadaljnji razvoj umetne inteligence.

Z izkoriščanjem zmogljivosti EU za naložbe v tehnologije in infrastrukturo naslednje generacije ter v digitalne kompetence, kot je podatkovna pismenost, se bo povečala tehnološka suverenost Evrope pri

[7] Čeprav bodo za preprečevanje zlorabe umetne inteligence za kazniva dejanja in boj proti njeni zlorabi morda potrebne nadaljnje ureditve, te presegajo področje te bele knjige.
[8] COM(2019) 168 final.

ključnih omogočitvenih tehnologijah in infrastrukturah podatkovnega gospodarstva. Infrastrukture bi morale podpirati oblikovanje evropskih zbirk podatkov, ki omogočajo zaupanja vredno umetno inteligenco, na primer umetno inteligenco, ki temelji na evropskih vrednotah in pravilih.

Evropa bi morala izkoristiti svoje prednosti za razširitev svojega vpliva na tem področju in vzdolž vrednostne verige, od sektorjev za proizvodnjo določene strojne opreme do programske opreme in vse do storitev. To v določenem obsegu že poteka. Evropa proizvede več kot četrtino vseh industrijskih in obrtnih strežnih robotov (na primer za precizno kmetovanje, varnost, zdravje, logistiko) in ima pomembno vlogo pri razvoju in uporabi programskih aplikacij za podjetja in organizacije (aplikacije „podjetje-podjetje“, kot je programska oprema za načrtovanje virov podjetja ter oblikovalska in inženirska programska oprema) ter aplikacij za podporo e-upravi in „inteligentnim podjetjem“.

Evropa je vodilna pri uvajanju umetne inteligence v proizvodnji. Več kot polovica največjih proizvajalcev na vsaj eni stopnji proizvodnih dejavnosti uporablja umetno inteligenco[9].

Eden od razlogov za močen položaj Evrope na področju raziskav je program financiranja EU, ki se je izkazal za ključnega pri združevanju dejavnosti, preprečevanju podvajanja ter spodbujanju javnih in zasebnih naložb v državah članicah. Sredstva EU, namenjena raziskavam in inovacijam na področju umetne inteligence, so se v zadnjih treh letih povečala za 70 % v primerjavi s prejšnjim obdobjem, in sicer na 1,5 milijarde evrov.

Vendar so naložbe v raziskave in inovacije v Evropi še vedno zelo majhne v primerjavi z javnimi in zasebnimi naložbami v drugih regijah sveta. V letu 2016 je bilo v umetno inteligenco v Evropi vloženih približno 3,2 milijarde evrov, medtem ko so naložbe v Severni Ameriki znašale približno 12,1 milijarde evrov, v Aziji pa približno 6,5 milijarde evrov[10]. Evropa mora zato svoje naložbe znatno povečati. Usklajeni načrt za umetno inteligenco[11], pripravljen z državami članicami, se je izkazal kot dobro izhodišče za tesnejše sodelovanje na področju umetne inteligence v Evropi in ustvarjanje sinergij, da bi se kar najbolj povečale naložbe v vrednostno verigo umetne inteligence.

3. IZKORIŠČANJE PRILOŽNOSTI PRED NAMI: NASLEDNJI PODATKOVNI VAL

Čeprav je Evropa trenutno v šibkejšem položaju na področju potrošnikovih aplikacij in spletnih platform, zaradi česar ima slabši konkurenčni položaj pri dostopu do podatkov, smo v vseh sektorjih priča velikim spremembam na področju vrednosti in ponovne uporabe podatkov. Količina podatkov, ustvarjenih na svetovni ravni, se hitro povečuje; leta 2018 je znašala 33 zetabajtov, do leta 2025 pa naj bi se povzpela na 175 zetabajtov.[12] Vsak nov val podatkov prinaša Evropi priložnosti, da najde svoje mesto v podatkovno okretnem gospodarstvu in postane vodilna v svetu na tem področju. V naslednjih petih letih se bo tudi bistveno spremenil način shranjevanja in obdelave podatkov. Danes 80 % obdelave in analize podatkov poteka v oblaku v podatkovnih centrih in centraliziranih računalniških zmogljivostih, 20 % pa v pametnih povezanih predmetih, kot so avtomobili, gospodinjske naprave ali industrijski roboti, in v računalniških zmogljivostih blizu uporabnikov („računalništvo na robu“). Do leta 2025 se bo to razmerje močno spremenilo[13].

Evropa je vodilna v svetu na področju elektronike z nizko porabo energije, ki je ključna za naslednjo generacijo specializiranih procesorjev za umetno inteligenco. Na tem trgu so trenutno vodilni

[9] Sledijo ji Japonska (30 %) in ZDA (28 %). Vir: CapGemini, 2019.
[10] *10 imperatives for Europe in the age of AI and automation* (10 prednostnih nalog za Evropo v dobi umetne inteligence in avtomatizacije), McKinsey, 2017.
[11] COM(2018) 795.
[12] IDC, 2019.
[13] Gartner, 2017.

neevropski akterji. To bi se lahko spremenilo s pomočjo pobud, kot je pobuda za evropske procesorje, ki se osredotoča na razvoj računalniških sistemov z nizko porabo energije za računalništvo na robu in visokozmogljivostno računalništvo naslednje generacije, ter delom v okviru skupnega podjetja za ključne digitalne tehnologije, ki naj bi se začelo leta 2021. Evropa je vodilna tudi pri nevromorfičnih rešitvah[14], ki so najprimernejše za avtomatizacijo industrijskih procesov (industrija 4.0) in načinov prevoza ter lahko izboljšajo energetsko učinkovitost za več redov velikosti.

Z nedavnim napredkom pri kvantnem računalništvu se bodo obdelovalne zmogljivosti eksponentno povečale[15]. Evropa je lahko na čelu te tehnologije zahvaljujoč svojim akademskim prednostim na področju kvantnega računalništva ter močnemu položaju evropske industrije pri kvantnih simulatorjih in programskih okoljih za kvantno računalništvo. Evropske pobude, katerih cilj je povečati razpoložljivost obratov za kvantno preskušanje in poskuse, bodo pomagale pri uporabi teh novih kvantnih rešitev v številnih industrijskih in akademskih sektorjih.

Hkrati bo Evropa še naprej v ospredju napredka pri algoritemskih temeljih umetne inteligence, pri čemer se bo opirala na lastno znanstveno odličnost. Zgraditi moramo mostove med strokami, ki trenutno delujejo ločeno, kot so strojno in globoko učenje (za katera so značilni omejena interpretabilnost, velika količina potrebnih podatkov za učenje modelov ter učenje s korelacijami) ter simbolični pristopi (pri katerih se pravila oblikujejo s človekovim posredovanjem). Kombiniranje simboličnega sklepanja z globokimi nevronskimi mrežami nam lahko pomaga izboljšati razložljivost rezultatov umetne inteligence.

4. EKOSISTEM ODLIČNOSTI

Za vzpostavitev ekosistema odličnosti, ki lahko podpre razvoj in uporabo umetne inteligence v celotnem gospodarstvu EU in javni upravi, je treba okrepiti ukrepanje na več ravneh.

A. SODELOVANJE Z DRŽAVAMI ČLANICAMI

Komisija je v skladu s svojo strategijo za umetno inteligenco, sprejeto aprila 2018[16], decembra 2018 predstavila usklajeni načrt, ki ga je z državami članicami pripravila za spodbujanje razvoja in uporabe umetne inteligence v Evropi[17].

V tem načrtu je predlaganih približno 70 skupnih ukrepov za tesnejše in učinkovitejše sodelovanje med državami članicami in Komisijo na ključnih področjih, kot so raziskave, naložbe, uvajanje na trg, spretnosti in talenti, podatki in mednarodno sodelovanje. Načrt naj bi se izvajal do leta 2027, pri čemer se bo redno spremljal in pregledoval.

Cilj je čim bolj povečati učinek naložb v raziskave, inovacije in uvajanje, oceniti nacionalne strategije za umetno inteligenco ter z državami članicami nadgraditi in razširiti usklajeni načrt za umetno inteligenco:

- *Ukrep 1: Komisija bo ob upoštevanju rezultatov javnega posvetovanja o beli knjigi državam članicam predlagala revizijo usklajenega načrta, ki naj bi bil sprejet do konca leta 2020.*

[14] Nevromorfične rešitve pomenijo vsak zelo obsežen sistem integriranih vezij, ki posnema nevrobiološke strukture, prisotne v živčnem sistemu.

[15] Kvantni računalniki bodo lahko v manj kot nekaj sekundah obdelali znatno večje nabore podatkov kot današnji najzmogljivejši računalniki, kar bo omogočilo razvoj novih aplikacij umetne inteligence v vseh sektorjih.

[16] Umetna inteligenca za Evropo (COM(2018) 237).

[17] Usklajeni načrt za umetno inteligenco (COM(2018) 795).

Financiranje umetne inteligence na ravni EU bi moralo pritegniti in združevati naložbe na področjih, na katerih potrebni ukrepi presegajo tisto, kar lahko posamezne države članice dosežejo same. Cilj je v naslednjih desetih letih v EU privabiti skupne naložbe v umetno inteligenco v višini več kot 20 milijard evrov[18] na leto. EU bo za spodbujanje zasebnih in javnih naložb zagotovila sredstva iz programa za digitalno Evropo, programa Obzorje Evropa ter evropskih strukturnih in investicijskih skladov, da bi se obravnavale potrebe manj razvitih regij in podeželskih območij.

Usklajeni načrt bi lahko kot ključni načeli umetne inteligence obravnaval tudi družbeno in okoljsko dobrostanje. Sistemi umetne inteligence obetajo pomoč pri reševanju najbolj perečih vprašanj, vključno s podnebnimi spremembami in degradacijo okolja. Vendar je pomembno, da k temu prispevajo na okolju prijazen način. Umetna inteligenca je sposobna in bi morala sama kritično preučiti porabo virov in energije ter bi jo bilo treba naučiti, da sprejema odločitve, ki imajo pozitiven vpliv na okolje. Komisija bo skupaj z državami članicami proučila možnosti za spodbujanje rešitev umetne inteligence, ki to upoštevajo.

B. OSREDOTOČANJE PRIZADEVANJ RAZISKOVALNE IN INOVACIJSKE SKUPNOSTI

Evropa si ne more privoščiti, da bi ohranila sedanjo razdrobljenost kompetenčnih centrov, od katerih nobeden ne dosega potrebne velikosti, da bi lahko konkuriral vodilnim inštitutom na svetovni ravni. Da bi lahko izboljšali odličnost, ohranili in privabili najboljše raziskovalce ter razvili najboljšo tehnologijo, moramo nujno ustvariti več sinergij in mrež med več evropskimi raziskovalnimi centri za umetno inteligenco in uskladiti njihova prizadevanja. Evropa potrebuje vodilni center za raziskave, inovacije in strokovno znanje, ki bi usklajeval ta prizadevanja in postal zgled odličnosti na področju umetne inteligence v svetu ter bi lahko privabil naložbe in največje talente.

Centri in mreže bi se morali osredotočiti na sektorje, v katerih ima Evropa potencial, da postane najuspešnejša na svetu, kot so industrija, zdravstvo, promet, finance, živilskopredelovalne vrednostne verige, energija/okolje, gozdarstvo, opazovanje Zemlje in vesolje. Na vseh teh področjih se odvija tekma za vodilno vlogo v svetu, Evropa pa ima znaten potencial, strokovno znanje in izkušnje[19]. Enako pomembno je, da se ustvarijo obrati za preskušanje in eksperimentiranje, s katerimi se bosta podprla razvoj in poznejše uvajanje novih aplikacij umetne inteligence.

- *Ukrep 2: Komisija bo olajšala ustanavljanje centrov odličnosti in centrov za preskušanje, ki lahko združijo evropske, nacionalne in zasebne naložbe, po možnosti z vključitvijo novega pravnega instrumenta. Komisija je predlagala, da se znotraj večletnega finančnega okvira za obdobje 2021–2027 znaten znesek iz programa za digitalno Evropo nameni ustanavljanju centrov za preskušanje v Evropi, ki bi bili zgled v svetovnem merilu. Ta znesek bo po potrebi dopolnjen z ukrepi na področju raziskav in inovacij v okviru programa Obzorje Evropa.*

C. SPRETNOSTI

Evropski pristop k umetni inteligenci bo moral temeljiti na močni osredotočenosti na spretnosti, da se zapolnijo vrzeli v kompetencah[20]. Komisija bo kmalu predstavila okrepljen program znanj in spretnosti, katerega cilj je zagotoviti, da bodo vsi Evropejci in Evropejke lahko izkoristili prednosti

[18] COM(2018) 237.

[19] Tudi prihodnji Evropski obrambni sklad in stalno strukturirano sodelovanje bosta zagotovila priložnosti za raziskave in razvoj na področju umetne inteligence. Te projekte bi bilo treba uskladiti s širšimi civilnimi programi EU, namenjenimi umetni inteligenci.

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

zelene in digitalne preobrazbe gospodarstva EU. Pobude bi lahko vključevale tudi podporo sektorskim regulatorjem, da bi se izboljšale njihove spretnosti na področju umetne inteligence, kar bi jim pomagalo pri učinkovitem in uspešnem izvajanju ustreznih pravil. Posodobljeni akcijski načrt za digitalno izobraževanje bo pripomogel k boljši uporabi podatkov in tehnologij, ki temeljijo na umetni inteligenci, kot sta učna in napovedna analitika, s čimer naj bi se izboljšali izobraževalni sistemi in sistemi usposabljanja ter se pripravili na digitalno dobo. Načrt bo prav tako povečal ozaveščenost o umetni inteligenci na vseh ravneh izobraževanja, da bi se državljanke in državljani pripravili na informirane odločitve, na katere bo vse bolj vplivala umetna inteligenca.

Razvoj spretnosti in znanj, potrebnih za delo na področju umetne inteligence, ter strokovno izpopolnjevanje delovne sile, da bo pripravljena na preobrazbo, ki jo prinaša umetna inteligenca, bosta prednostni nalogi revidiranega usklajenega načrta za umetno inteligenco, ki bo razvit v sodelovanju z državami članicami. To bi lahko vključevalo preoblikovanje ocenjevalnega seznama na podlagi etičnih smernic v okvirni „učni načrt“ za razvijalce umetne inteligence, ki bo kot vir na voljo ustanovam za usposabljanje. Posebej si je treba prizadevati za povečanje števila žensk, ki se usposabljajo in so zaposlene na tem področju.

Poleg tega bi vodilni center za raziskave in inovacije na področju umetne inteligence v Evropi zaradi možnosti, ki bi jih lahko ponujal, lahko pritegnil talente z vsega sveta. Razvijal in širil bi tudi odličnost pri spretnostih, ki bi se lahko ukoreninile in razrasle po vsej Evropi.

- *Ukrep 3: S stebrom naprednih spretnosti programa za digitalno Evropo vzpostaviti in podpirati mreže vodilnih univerz in visokošolskih ustanov, da bi pritegnili najboljše profesorje in znanstvenike ter ponujali magistrske programe na področju umetne inteligence, ki bi bili vodilni v svetu.*

Poleg strokovnega izpopolnjevanja na delovnem mestu na zaposlene neposredno vplivata tudi načrtovanje in uporaba sistemov umetne inteligence. Vključenost socialnih partnerjev bo odločilni dejavnik pri zagotavljanju humanocentričnega pristopa k umetni inteligenci na delovnem mestu.

D. OSREDOTOČENOST NA MSP

Pomembno bo zagotoviti, da lahko do umetne inteligence dostopajo in jo uporabljajo tudi MSP. V ta namen bi bilo treba nadalje okrepiti vozlišča digitalnih inovacij[21] in platformo za umetno inteligenco na zahtevo[22] ter spodbujati sodelovanje med MSP. V ta namen bo bistvenega pomena program za digitalno Evropo. Čeprav bi morala vsa vozlišča digitalnih inovacij zagotavljati podporo MSP pri razumevanju in sprejemanju umetne inteligence, je pomembno, da je vsaj eno inovacijsko vozlišče v vsaki državi članici visoko specializirano za umetno inteligenco.

MSP in zagonska podjetja bodo potrebovala dostop do financiranja, da bodo lahko svoje procese prilagodila umetni inteligenci oziroma inovirala z njeno uporabo. Komisija namerava na podlagi prihodnjega pilotnega sklada za naložbe v umetno inteligenco in blokovno verigo, vrednega 100 milijonov evrov, še povečati dostop do financiranja za umetno inteligenco v okviru programa InvestEU[23]. Umetna inteligenca je izrecno navedena med področji, ki so upravičena do uporabe jamstva InvestEU.

[21] https://ec.europa.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities
[22] www.Ai4eu.eu.
[23] Europa.eu/investeu/home_sl.

- *Ukrep 4: Komisija bo sodelovala z državami članicami, da bi zagotovila, da je v vsaki državi članici vsaj eno vozlišče digitalnih inovacij visoko specializirano za umetno inteligenco. Vozlišča digitalnih inovacij se lahko podprejo v okviru programa za digitalno Evropo.*
- *Komisija in Evropski investicijski sklad bosta v prvem četrtletju leta 2020 začela izvajati pilotni program v vrednosti 100 milijonov evrov, ki bo zagotovil lastniško financiranje za inovativen razvoj na področju umetne inteligence. Komisija namerava ta pilotni program od leta 2021 znatno razširiti prek programa InvestEU s pridržkom končnega dogovora o večletnem finančnem okviru.*

E. PARTNERSTVO Z ZASEBNIM SEKTORJEM

Ključnega pomena je tudi to, da se zasebni sektor v celoti vključi v pripravo načrta za raziskave in inovacije ter prispeva potreben delež naložb. Zato je treba vzpostaviti široko zastavljeno javno-zasebno partnerstvo in zagotoviti zavezanost najvišjega vodstva podjetij.

- *Ukrep 5: Komisija bo v okviru programa Obzorje Evropa vzpostavila novo javno-zasebno partnerstvo na področju umetne inteligence, podatkov in robotike, da bi združila prizadevanja in zagotovila usklajevanje raziskav in inovacij na področju umetne inteligence, in sodelovala z drugimi javno-zasebnimi partnerstvi v okviru programa Obzorje Evropa ter zgoraj navedenimi centri za preskušanje in vozlišči digitalnih inovacij.*

F. SPODBUJANJE UPORABE UMETNE INTELIGENCE V JAVNEM SEKTORJU

Bistvenega pomena je, da javne uprave, bolnišnice, službe za zagotavljanje komunalnih storitev in javnega prevoza, finančni nadzorniki in druge službe v javnem interesu v svoje dejavnosti hitro začnejo uvajati proizvode in storitve, ki temeljijo na umetni inteligenci. Posebna pozornost bo namenjena področjem zdravstvenega varstva in prometa, na katerih je ustrezna tehnologija zrela za obsežno uvedbo.

- *Ukrep 6: Komisija bo uvedla odprte in pregledne sektorske dialoge, pri čemer bo prednost namenila zdravstvenemu varstvu, podeželskim upravam in izvajalcem javnih služb, da bi predstavila akcijski načrt za spodbujanje razvoja umetne inteligence, eksperimentiranja z njo in njenega sprejemanja. Sektorski dialogi se bodo uporabili za pripravo posebnega „programa za sprejemanje umetne inteligence“, ki bo podpiral javno naročanje sistemov umetne inteligence in pomagal pri preoblikovanju samih postopkov javnega naročanja.*

G. ZAGOTAVLJANJE DOSTOPA DO PODATKOV IN RAČUNALNIŠKE INFRASTRUKTURE

Področja ukrepanja, navedena v tej beli knjigi, dopolnjujejo vzporedno predstavljen načrt v okviru evropske podatkovne strategije. Izboljšanje dostopa do podatkov in njihovega upravljanja je bistvenega pomena, saj razvoj umetne inteligence in drugih digitalnih aplikacij brez podatkov ni mogoč. Ogromen obseg novih podatkov, ki bodo ustvarjeni v prihodnosti, je priložnost, da Evropa prevzame vodilno vlogo na področju podatkovne in umetnointeligenčne preobrazbe. Spodbujanje odgovornih praks ravnanja s podatki in skladnosti podatkov z načeli FAIR bo prispevalo k vzpostavitvi zaupanja in zagotovilo možnost ponovne uporabe podatkov[24]. Enako pomembne so naložbe v ključne računalniške tehnologije in infrastrukture.

Komisija je predlagala, da se v okviru programa za digitalno Evropo več kot 4 milijarde evrov namenijo podpori visokozmogljivostnemu in kvantnemu računalništvu, vključno z računalništvom na robu in umetno inteligenco ter podatkovno infrastrukturo in infrastrukturo v oblaku. Te prednostne naloge nadalje razvija evropska podatkovna strategija.

H. MEDNARODNI VIDIKI

Evropa je v dobrem položaju, da ohrani največji vpliv v svetu pri sklepanju zavezništev na podlagi skupnih vrednot in spodbujanju etične uporabe umetne inteligence. Delo EU na področju umetne inteligence že vpliva na mednarodne razprave. Strokovna skupina na visoki ravni je v pripravo etičnih smernic vključila številne organizacije, ki niso iz EU, in več vladnih opazovalcev. Obenem je EU tesno sodelovala pri razvoju etičnih načel OECD za umetno inteligenco[25]. Skupina G20 je nato podprla ta načela v Ministrski izjavi o trgovini in digitalnem gospodarstvu iz junija 2019.

EU hkrati priznava, da pomembno delo na področju umetne inteligence poteka tudi v drugih večstranskih forumih, med drugim v Svetu Evrope, Organizaciji Združenih narodov za izobraževanje, znanost in kulturo (UNESCO), Organizaciji za gospodarsko sodelovanje in razvoj (OECD), Svetovni trgovinski organizaciji in Mednarodni telekomunikacijski zvezi (ITU). V okviru ZN je EU vključena v nadaljnje ukrepanje na podlagi poročila skupine na visoki ravni za digitalno sodelovanje, vključno s priporočilom skupine o umetni inteligenci.

---

[24] Podatke je mogoče najti, so dostopni in interoperabilni ter se lahko ponovno uporabijo (Findable, Accessible, Interoperable and Reusable), kot je navedeno v končnem poročilu in akcijskem načrtu skupine strokovnjakov Komisije za podatke FAIR iz leta 2018: https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

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

EU bo še naprej sodelovala s podobno mislečimi državami, pa tudi s svetovnimi akterji na področju umetne inteligence, pri čemer bo sledila pristopu, ki temelji na pravilih in vrednotah EU (na primer podpiranje regulativnega zbliževanja k višjim standardom, dostop do ključnih virov, vključno s podatki, ustvarjanje enakih konkurenčnih pogojev). Komisija bo pozorno spremljala politike tretjih držav, ki omejujejo pretok podatkov, ter v dvostranskih trgovinskih pogajanjih in z ukrepi v okviru Svetovne trgovinske organizacije obravnavala neupravičene omejitve. Prepričana je, da mora mednarodno sodelovanje pri zadevah umetne inteligence temeljiti na pristopu, ki spodbuja spoštovanje temeljnih pravic, vključno s človekovim dostojanstvom, pluralizmom, vključevanjem, nediskriminacijo in varstvom zasebnosti in osebnih podatkov[26], ter si bo prizadevala za izvoz svojih vrednot po svetu[27]. Prav tako je jasno, da je odgovoren razvoj in uporaba umetne inteligence lahko gonilna sila za doseganje ciljev trajnostnega razvoja in uresničevanje Agende 2030.

5. EKOSISTEM ZAUPANJA: REGULATIVNI OKVIR ZA UMETNO INTELIGENCO

Kot vsaka nova tehnologija tudi umetna inteligenca prinaša tako priložnosti kot tveganja. Kar zadeva asimetričnost informacij pri algoritemskem odločanju, so državljanke in državljani zaskrbljeni, da ne bodo več mogli zaščititi svojih pravic in varnosti, podjetja pa skrbi pravna negotovost. Umetna inteligenca sicer lahko pomaga zaščititi varnost državljank in državljanov ter jim lahko omogoča uživanje temeljnih pravic, vendar obstajajo tudi pomisleki glede morebitnih neželenih učinkov ali celo zlonamerne uporabe umetne inteligence. Te pomisleke moramo obravnavati. Poleg pomanjkanja naložb in spretnosti je glavni dejavnik, ki ovira širšo uporabo umetne inteligence, pomanjkanje zaupanja.

Komisija je zato 25. aprila 2018 določila strategijo za umetno inteligenco[28], ki obravnava socialnoekonomske vidike vzporedno s povečanjem naložb v raziskave, inovacije in zmogljivost umetne inteligence po vsej EU. Z državami članicami se je dogovorila tudi o usklajenem načrtu[29] za uskladitev njihovih strategij. Prav tako je ustanovila strokovno skupino na visoki ravni, ki je aprila 2019 objavila smernice za zaupanja vredno umetno inteligenco[30].

Komisija je objavila sporočilo[31], v katerem je pozdravila sedem ključnih zahtev iz smernic strokovne skupine na visoki ravni:

- človekovo delovanje in nadzor,
- tehnična robustnost in varnost,
- zasebnost in upravljanje podatkov,
- preglednost,
- raznolikost, nediskriminacija in pravičnost,
- okoljska in družbena blaginja ter
- odgovornost.

Poleg tega smernice vsebujejo ocenjevalni seznam za uporabo v praksi, namenjen podjetjem. V drugi polovici leta 2019 je ta ocenjevalni seznam preskusilo več kot 350 organizacij, ki so poslale povratne

[26] Komisija bo v okviru instrumenta partnerstva financirala projekt v vrednosti 2,5 milijona evrov, ki bo olajšal sodelovanje s podobno mislečimi partnerji, da bi se spodbujale etične smernice EU za umetno inteligenco ter sprejela skupna načela in operativni sklepi.

[27] Predsednica von der Leyen, Bolj ambiciozna Unija – Moj načrt za Evropo, str. 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.

informacije. Skupina na visoki ravni zdaj revidira svoje smernice na podlagi teh povratnih informacij, revizijo naj bi zaključila do junija 2020. Ključna ugotovitev na podlagi povratnih informacij je to, da kljub temu, da so v obstoječih pravnih ali regulativnih ureditvah že zajete številne zahteve, v mnogih gospodarskih sektorjih sedanja zakonodaja ne vključuje zahtev glede preglednosti, sledljivosti in človekovega nadzora.

V skladu s političnimi usmeritvami predsednice bi, poleg tega sklopa nezavezujočih smernic strokovne skupine na visoki ravni, jasen evropski regulativni okvir okrepil zaupanje potrošnikov in podjetij v umetno inteligenco ter s tem pospešil uporabo te tehnologije. Takšen regulativni okvir bi moral biti skladen z drugimi ukrepi za spodbujanje evropske inovacijske zmogljivosti in konkurenčnosti na tem področju. Prav tako mora zagotoviti najboljše možne rezultate z družbenega, okoljskega in ekonomskega vidika ter skladnost z zakonodajo, načeli in vrednotami EU. To je zlasti pomembno na področjih, na katerih je vpliv na pravice državljank in državljanov lahko najbolj neposreden, na primer pri uporabi umetne inteligence za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in pravosodje.

Za razvijalce in uvajalce umetne inteligence že veljajo evropska zakonodaja o temeljnih pravicah (na primer varstvo podatkov, zasebnost, nediskriminacija) in varstvu potrošnikov ter pravila o varnosti proizvodov in odgovornosti. Potrošniki pričakujejo enako raven varnosti in spoštovanja pravic, ne glede na to, ali proizvod ali sistem temelji na umetni inteligenci. Vendar pa lahko nekatere posebne značilnosti umetne inteligence (na primer nepreglednost) otežijo uporabo in izvrševanje te zakonodaje. Zato je treba preučiti, ali sedanja zakonodaja lahko obravnava tveganja umetne inteligence in se učinkovito izvršuje oziroma ali jo je potrebno prilagoditi ali nadomestiti z novo.

Glede na to, kako hitro se umetna inteligenca razvija, mora regulativni okvir dopuščati prostor za prihodnji razvoj. Vsakršne spremembe bi morale biti omejene na jasno opredeljene težave, za katere obstajajo izvedljive rešitve.

Države članice opozarjajo, da trenutno ni skupnega evropskega okvira. Nemška komisija za etiko podatkov je pozvala k petstopenjskemu sistemu, ki temelji na tveganju in zajema vse od popolne neregulacije za najbolj neškodljive sisteme umetne inteligence do popolne prepovedi najnevarnejših sistemov. Danska je pravkar uvedla prototip pečata etičnih podatkov, Malta pa je uvedla prostovoljni sistem certificiranja umetne inteligence. Če EU ne zagotovi pristopa na ravni EU, obstaja resnično tveganje razdrobljenosti notranjega trga, ki bi ogrozila cilje zaupanja, pravne varnosti in uvajanja na trg.

Trden evropski regulativni okvir za zaupanja vredno umetno inteligenco bo zaščitil vse evropske državljanke in državljane, pomagal ustvariti notranji trg brez motenj za nadaljnji razvoj in uporabo umetne inteligence ter okrepil evropsko industrijsko bazo na področju umetne inteligence.

A. OPREDELITEV PROBLEMA

Medtem ko lahko umetna inteligenca prinese veliko dobrega, med drugim varnejše proizvode in postopke, lahko povzroči tudi škodo. Ta škoda je lahko tako stvarna (varnost in zdravje posameznikov, vključno s smrtjo, škoda na premoženju) kot tudi nestvarna (izguba zasebnosti, omejitev svobode izražanja in spoštovanja človekovega dostojanstva, diskriminacija, na primer pri dostopu do zaposlitve) in povezana z najrazličnejšimi tveganji. Regulativni okvir bi moral biti osredotočen na to, kako čim bolj zmanjšati različna tveganja za morebitno škodo, zlasti najresnejša.

Glavna tveganja, povezana z uporabo umetne inteligence, se nanašajo na uporabo pravil o varstvu temeljnih pravic (vključno z varstvom osebnih podatkov in zasebnosti ter načelom nediskriminacije), pa tudi na vprašanja v zvezi z varnostjo[32] in odgovornostjo.

Tveganja za temeljne pravice, vključno z varstvom osebnih podatkov in zasebnosti ter nediskriminacijo

Uporaba umetne inteligence lahko vpliva na vrednote, na katerih temelji EU, in vodi v kršitve temeljnih pravic [33], vključno s pravico do svobode izražanja, svobode zbiranja, človekovega dostojanstva, nediskriminacije na podlagi spola, rase ali narodnosti, verskega ali drugega prepričanja, invalidnosti, starosti ali spolne usmerjenosti, kot veljajo na nekaterih področjih, pravico do varstva osebnih podatkov in zasebnega življenja[34] ter pravico do učinkovitega pravnega sredstva in poštenega sojenja, vpliva pa lahko tudi na varstvo potrošnikov. Ta tveganja lahko izhajajo iz pomanjkljivosti v splošni zasnovi sistemov umetne inteligence (tudi kar zadeva človekov nadzor) ali iz uporabe podatkov, ne da bi se odpravila morebitna pristranskost (na primer sistem se uči samo z uporabo podatkov o moških, zaradi česar so rezultati v zvezi z ženskami neoptimalni).

Umetna inteligenca lahko opravlja številne naloge, ki so jih prej lahko opravljali samo ljudje. Zato bodo sistemi umetne inteligence vedno pogosteje sprejemali ali pomagali sprejemati ukrepe in odločitve o državljanih in pravnih subjektih, ki jih je včasih težko razumeti in učinkovito izpodbijati, kadar je to potrebno. Umetna inteligenca poleg tega povečuje možnosti za spremljanje in analiziranje vsakodnevnih navad ljudi. Eno od možnih tveganj je recimo, da bi državni organi ali drugi subjekti umetno inteligenco uporabljali za množični nadzor, kar je v nasprotju s pravili EU o varstvu podatkov in drugimi pravili, delodajalci pa za opazovanje svojih zaposlenih. Z analizo velikih količin podatkov in ugotavljanjem povezav med njimi se lahko umetna inteligenca uporabi tudi za izsledite in deanonimizacijo podatkov o osebah, kar ustvarja nova tveganja za varstvo osebnih podatkov, tudi pri naborih podatkov, ki sami po sebi ne vključujejo osebnih podatkov. Umetno inteligenco uporabljajo tudi spletni posredniki, da prednostno razvrstijo informacije za svoje uporabnike in za urejanje vsebin. Obdelani podatki, način zasnovanja aplikacij in obseg človekovega posredovanja lahko vplivajo na pravice do svobodnega izražanja, varstva osebnih podatkov, zasebnosti in političnih svoboščin.

[32] To vključuje vprašanja kibernetske varnosti, uporabe umetne inteligence v kritični infrastrukturi in zlonamerne uporabe umetne inteligence.

[33] Raziskave Sveta Evrope kažejo, da bi lahko uporaba umetne inteligence vplivala na številne temeljne pravice: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

[34] Splošna uredba o varstvu podatkov in direktiva o zasebnosti in elektronskih komunikacijah (o novi uredbi o e-zasebnosti potekajo pogajanja) obravnavata ta tveganja, vendar bi bilo morda treba preučiti, ali sistemi umetne inteligence predstavljajo dodatna tveganja. Komisija bo stalno spremljala in ocenjevala uporabo splošne uredbe o varstvu podatkov.

Nekateri algoritmi umetne inteligence, ki se uporabljajo za napovedovanje povratništva, so lahko pristranski zaradi spola in rase, zaradi česar pride do razlik pri napovedovanju verjetnosti povratništva za ženske v primerjavi z moškimi ali za državljane v primerjavi s tujci. *Vir: 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 (Zakaj lahko strojno učenje vodi v nepravičnost: dokazi na podlagi ocene tveganja v sodstvu za mladoletnike v Kataloniji), nagrada za najboljše raziskovalno delo, mednarodna konferenca o umetni inteligenci in pravu, 2019.*

Nekateri programi umetne inteligence za analizo obraza so pristranski glede na spol in raso, saj je stopnja napak pri določanju spola moških svetlejše polti nizka, pri določanju spola žensk temnejše polti pa visoka. Vir: *Joy Buolamwini, Timnit Gebru: Proceedings of the 1st Conference on Fairness, Accountability and Transparency (Izidi 1. konference o pravičnosti, odgovornosti in preglednosti), PMLR 81:77–91, 2018.*

Tveganje pristranskosti in diskriminacije sta sestavna dela vsake družbene ali gospodarske dejavnosti. Človekove odločitve niso imune za napake in predsodke. Vendar bi enaka pristranskost pri umetni inteligenci lahko imela veliko večji učinek in zaradi diskriminacije bi lahko bilo prizadetih veliko ljudi, saj ta ne vključuje mehanizmov družbenega nadzora, ki vodijo človekovo vedenje[35]. Do tega lahko pride tudi pri „učenju“ sistema umetne inteligence med delovanjem. V takih primerih, kadar rezultata ni bilo mogoče preprečiti ali predvideti v fazi zasnove, tveganja ne izhajajo iz pomanjkljivosti v prvotni zasnovi sistema, temveč iz praktičnih učinkov korelacij ali vzorcev, ki jih sistem prepozna v velikem naboru podatkov.

Zaradi posebnih značilnosti številnih tehnologij umetne inteligence, vključno z nepreglednostjo (t. i. učinek črne skrinjice), kompleksnostjo, nepredvidljivostjo in delno avtonomnim vedenjem, bo morda težko preverjati skladnost s pravili veljavne zakonodaje EU za varstvo temeljnih pravic, učinkovito izvrševanje teh pravil pa bi bilo lahko ovirano. Izvršilni organi in prizadeti posamezniki morda ne bodo mogli preveriti, kako je bila odločitev z uporabo umetne inteligence sprejeta, prav tako pa ne tega, ali so bila upoštevana ustrezna pravila. Posamezniki in pravni subjekti se bodo morda soočali s težavami pri učinkovitem dostopu do pravnega varstva v primerih, ko bi lahko take odločitve nanje negativno vplivale.

Tveganja za varnost in učinkovito delovanje ureditve odgovornosti

Tehnologije umetne inteligence lahko prinašajo nova varnostna tveganja za uporabnike, če so vgrajene v proizvode in storitve. Zaradi napake v tehnologiji prepoznavanja predmetov lahko avtonomni avtomobil na primer napačno prepozna predmet na cesti in povzroči nesrečo s poškodbami in premoženjsko škodo. Tako kot tveganja za temeljne pravice so lahko tudi ta tveganja posledica pomanjkljivosti v zasnovi tehnologije umetne inteligence, povezana pa so lahko s težavami z razpoložljivostjo in kakovostjo podatkov ali z drugimi težavami, ki izhajajo iz strojnega učenja. Čeprav nekatera od teh tveganj niso omejena na proizvode in storitve, ki temeljijo na umetni inteligenci, lahko uporaba umetne inteligence poveča ali razširi tveganje.

[35] Svetovalni odbor Komisije za enake možnosti žensk in moških trenutno pripravlja „Mnenje o umetni inteligenci“, v katerem bodo med drugim preučeni učinki umetne inteligence na enakost spolov in ki naj bi ga Komisija sprejela v začetku leta 2020. Tudi strategija EU za enakost spolov za obdobje 2020–2024 obravnava povezavo med umetno inteligenco in enakostjo spolov. Evropska mreža organov za enakost (Equinet) bo objavila poročilo (Robina Allena in Dee Masters) z naslovom *Regulating AI: the new role for Equality Bodies – Meeting the new challenges to equality and non-discrimination from increased digitalisation and the use of AI* (Reguliranje umetne inteligence: nova vloga organov za enakost – Soočanje z novimi izzivi za enakost in nediskriminacijo zaradi vedno večje digitalizacije in uporabe umetne inteligence), ki naj bi bilo pripravljeno v začetku leta 2020.

Če ne obstajajo jasne varnostne določbe za obravnavanje teh tveganj, se lahko poleg tveganj za zadevne posameznike ustvari pravna negotovost za podjetja, ki v EU tržijo svoje proizvode, ki vključujejo umetno inteligenco. Organi za nadzor trga in izvršilni organi se lahko znajdejo v položaju, v katerem ni jasno, ali lahko posredujejo, saj morda niso pooblaščeni za ukrepanje in/ali nimajo ustreznih tehničnih zmogljivosti za inšpekcijo sistemov[36]. Pravna negotovost lahko torej zmanjša splošno raven varnosti in ogrozi konkurenčnost evropskih podjetij.

Če se varnostna tveganja uresničijo, je zaradi pomanjkanja jasnih zahtev in značilnosti tehnologij umetne inteligence, navedenih zgoraj, težko izslediti potencialno problematične odločitve, sprejete z uporabo sistemov umetne inteligence. To pa lahko osebam, ki so utrpele škodo, oteži pridobitev odškodnine na podlagi veljavne zakonodaje EU in nacionalne zakonodaje o odgovornosti[37].

V skladu z direktivo o odgovornosti za proizvode je proizvajalec odgovoren za škodo, ki jo povzroči proizvod z napako. Vendar je v primeru sistema, ki temelji na umetni inteligenci, kot so na primer avtonomni avtomobili, lahko težko dokazati napako na proizvodu, nastalo škodo in vzročno zvezo med njima. Poleg tega je nekoliko negotovo, kako in v kolikšni meri se direktiva o odgovornosti za proizvode uporablja v primeru nekaterih vrst napak, na primer če so te posledica pomanjkljivosti v kibernetski varnosti proizvoda.

Zato težava pri sledenju morebitnim problematičnim odločitvam, ki jih sprejmejo sistemi umetne inteligence in so navedene zgoraj v zvezi s temeljnimi pravicami, enako velja za vprašanja varnosti in odgovornosti. Osebe, ki so utrpele škodo, morda nimajo učinkovitega dostopa do dokazov, ki so potrebni za predložitev zadeve sodišču, njihove možnosti pravnih sredstev pa so lahko manj učinkovite kot v primerih, ko škodo povzročijo tradicionalne tehnologije. Ta tveganja bodo še večja, ko se bo uporaba umetne inteligence bolj razširila.

B. MOŽNE PRILAGODITVE OBSTOJEČEGA PRAVNEGA OKVIRA EU V ZVEZI Z UMETNO INTELIGENCO

Obsežen sklop obstoječe zakonodaje EU o varnosti proizvodov in odgovornosti[38], vključno s sektorskimi pravili, ki jo dodatno dopolnjuje nacionalna zakonodaja, je relevanten in ga je morda mogoče uporabiti za več nastajajočih aplikacij umetne inteligence.

[36] Primer za to je lahko pametna ura za otroke. Ta proizvod morda ne bi povzročil neposredne škode za otroka, ki ga nosi, toda brez zagotovljene minimalne ravni varnosti ga je mogoče z lahkoto uporabiti kot orodje za dostop do otroka. Organi za nadzor trga lahko morda le težko posredujejo v primerih, ko tveganje ni povezano s proizvodom kot takim.

[37] V poročilu Komisije, priloženem tej beli knjigi, so preučene posledice umetne inteligence, interneta stvari in drugih digitalnih tehnologij za zakonodajo o varnosti in odgovornosti.

[38] Pravni okvir EU za varnost proizvodov vključuje direktivo o splošni varnosti proizvodov (Direktiva 2001/95/ES) kot varnostno mrežo ter vrsto sektorskih pravil, ki veljajo za različne proizvode od strojev, letal in avtomobilov do igrač in medicinskih pripomočkov, s katerimi želi EU zagotoviti visoko raven zdravja in varnosti. Zakonodajo o odgovornosti za proizvode dopolnjujejo različne ureditve civilne odgovornosti za škodo, ki jo povzročijo proizvodi ali storitve.

V zvezi z varstvom temeljnih pravic in pravic potrošnikov zakonodajni okvir EU vključuje zakonodajne akte, kot so direktiva o rasni enakosti [39], direktiva o enakem obravnavanju pri zaposlovanju in delu [40], direktivi o enakem obravnavanju moških in žensk pri zaposlovanju ter dostopu do blaga in storitev[41], več pravil o varstvu potrošnikov[42] ter osebnih podatkov in zasebnosti, zlasti splošna uredba o varstvu podatkov, ter druga sektorska zakonodaja, ki pokriva varstvo osebnih podatkov, kot je direktiva o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj [43]. Leta 2025 pa se bodo začela uporabljati še pravila v zvezi z zahtevami glede dostopnosti za blago in storitve, določena v evropskem aktu o dostopnosti[44]. Poleg tega je pri izvajanju druge zakonodaje EU treba spoštovati temeljne pravice, tudi na področju finančnih storitev, migracij ali odgovornosti spletnih posrednikov.

Medtem ko se zakonodaja EU načeloma še naprej uporablja v celoti, ne glede na prisotnost umetne inteligence, je pomembno oceniti, ali jo je mogoče ustrezno izvrševati za obravnavo tveganj, ki jih ustvarjajo sistemi umetne inteligence, ali pa so potrebne prilagoditve specifičnih pravnih instrumentov.

Tako na primer gospodarski subjekti ostajajo v celoti odgovorni za skladnost umetne inteligence z obstoječimi pravili, ki ščitijo potrošnike. Vsakršno algoritemsko vrednotenje potrošnikovega vedenja, ki krši obstoječa pravila, ne bi smelo biti dovoljeno, kršitve pa bi morale biti ustrezno kaznovane.

Komisija meni, da bi bilo mogoče zakonodajni okvir izboljšati, da se obravnavajo naslednja tveganja in situacije:

- *Učinkovita uporaba in izvrševanje obstoječe zakonodaje EU in nacionalne zakonodaje*: ključne značilnosti umetne inteligence ustvarjajo izzive za zagotavljanje ustrezne uporabe in izvrševanja zakonodaje EU in nacionalne zakonodaje. Zaradi pomanjkanja preglednosti (nepreglednost umetne inteligence) je težko odkriti in dokazati morebitne kršitve zakonov, vključno s kršitvami pravnih določb, ki ščitijo temeljne pravice, nekomu pripisati kaznivo dejanje in izpolniti pogoje za odškodninski zahtevek. Zato bo za zagotovitev učinkovite uporabe in izvrševanja obstoječo zakonodajo morda treba prilagoditi ali pojasniti na nekaterih področjih, na primer glede odgovornosti, kot je podrobneje opisano v poročilu, ki je priloženo beli knjigi.

- *Omejitve področja uporabe obstoječe zakonodaje EU*: zakonodaja EU o varnosti proizvodov je osredotočena predvsem na dajanje proizvodov na trg. Medtem ko mora v skladu z zakonodajo EU o varnosti proizvodov programska oprema, ki je del končnega proizvoda, izpolnjevati ustrezna pravila o varnosti proizvodov, pa ostaja odprto vprašanje, ali zakonodaja EU o varnosti proizvodov pokriva samostojno programsko opremo, razen v nekaterih sektorjih z izrecnimi pravili[45]. Splošna trenutno veljavna zakonodaja EU o varnosti se uporablja za

[39] Direktiva 2000/43/ES.
[40] Direktiva 2000/78/ES.
[41] Direktiva 2004/113/ES; Direktiva 2006/54/ES.
[42] Kot sta direktiva o nepoštenih poslovnih praksah (Direktiva 2005/29/ES) in direktiva EU o pravicah potrošnikov (Direktiva 2011/83/ES).
[43] Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov.
[44] Direktiva (EU) 2019/882 o zahtevah glede dostopnosti za proizvode in storitve.
[45] Na primer, programska oprema, namenjena za uporabo v zdravstvene namene, se v skladu z uredbo o medicinskih pripomočkih (Uredba (EU) 2017/745) šteje za medicinski pripomoček.

proizvode in ne za storitve in tako načeloma tudi ne za storitve, ki temeljijo na tehnologiji umetne inteligence (npr. zdravstvene storitve, finančne storitve, transportne storitve).

- *Spreminjajoča se funkcionalnost sistemov umetne inteligence*: integracija programske opreme v proizvode, vključno z umetno inteligenco, lahko spremeni funkcionalnost takšnih proizvodov in sistemov tekom njihovega življenjskega cikla. To velja zlasti za sisteme, ki potrebujejo pogoste posodobitve programske opreme ali ki se zanašajo na stojno učenje. Te značilnosti lahko povzročijo nova tveganja, ki niso bila prisotna, ko je bil sistem dan na trg. Obstoječa zakonodaja, ki se osredotoča predvsem na varnostna tveganja, prisotna v času dajanja na trg, teh tveganj ne obravnava ustrezno.

- *Negotovost glede delitve odgovornosti med različnimi gospodarskimi subjekti v dobavni verigi*: zakonodaja EU o varnosti proizvodov običajno odgovornost nalaga proizvajalcu proizvoda, danega na trg, vključno z vsemi sestavnimi deli, npr. sistemi umetne inteligence. Vendar lahko ta pravila postanejo nejasna, če umetno inteligenco doda stran, ki ni proizvajalec, potem ko se proizvod da na trg. Poleg tega zakonodaja EU o odgovornosti za proizvode določa odgovornost proizvajalcev in dopušča, da odgovornost drugih v dobavni verigi urejajo nacionalna pravila o odgovornosti.

- *Spremembe koncepta varnosti*: uporaba umetne inteligence v proizvodih in storitvah lahko povzroči tveganja, ki jih zakonodaja EU trenutno izrecno ne obravnava. Ta tveganja so lahko povezana s kibernetskimi grožnjami, tveganji za osebno varnost (na primer v povezavi z novimi uporabami umetne inteligence, kot so gospodinjske naprave), tveganji, ki izhajajo iz izgube povezljivosti itd. Prisotna so lahko v času dajanja proizvodov na trg ali se pojavijo kot posledica posodobitev programske opreme ali samoučenja med uporabo proizvoda. EU bi za ocenjevanje groženj umetne inteligence morala v celoti uporabljati orodja, ki jih ima na razpolago, da izboljša bazo dokazov o morebitnih tveganjih, povezanih z aplikacijami umetne inteligence, vključno z upoštevanjem izkušenj Agencije EU za kibernetsko varnost (ENISA).

Kot je bilo že navedeno, več držav članic že raziskuje možnosti nacionalne zakonodaje za obravnavo izzivov, ki jih prinaša umetna inteligenca. To lahko vodi v razdrobljenost enotnega trga. Različna nacionalna pravila bodo verjetno ustvarila ovire za podjetja, ki želijo prodajati in upravljati sisteme umetne inteligence na enotnem trgu. Zagotavljanje skupnega pristopa na ravni EU bi evropskim podjetjem omogočalo, da izkoristijo nemoten dostop na enotni trg, ter bi pripomoglo k njihovi konkurenčnosti na globalnih trgih.

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

V poročilu, ki je priloženo tej beli knjigi, je analiziran ustrezni pravni okvir. V njem so opredeljene negotovosti glede uporabe tega okvira za specifična tveganja, ki jih predstavljajo sistemi umetne inteligence in druge digitalne tehnologije.

V poročilu se ugotavlja, da trenutna zakonodaja o varnosti proizvodov že podpira razširjen koncept varnosti, ki ščiti pred vsemi vrstami tveganj, ki nastanejo pri uporabi proizvoda. Vendar bi lahko uvedli določbe, ki bi izrecno pokrivale nova tveganja, ki jih prinašajo nove digitalne tehnologije, da se zagotovi večja pravna varnost.

- Avtonomno vedenje nekaterih sistemov umetne inteligence tekom njihovega življenjskega cikla lahko povzroči pomembne spremembe proizvoda, ki vplivajo na varnost, zaradi česar je lahko potrebna nova ocena tveganja. Poleg tega bo kot varovalo morda potreben človeški nadzor, in sicer vse od zasnove proizvodov ter skozi celotno življenjsko dobo proizvodov in sistemov umetne inteligence.
- O izrecnih obveznostih za proizvajalce velja po potrebi razmisliti tudi v zvezi s tveganji za duševno zdravje uporabnikov (npr. pri sodelovanju s humanoidnimi roboti).
- Zakonodaja Unije o varnosti proizvodov bi lahko določala specifične zahteve, ki obravnavajo varnostna tveganja zaradi napačnih podatkov v fazi oblikovanja proizvoda, ter mehanizme za zagotovitev, da se ves čas uporabe proizvodov in sistemov umetne inteligence ohranja kakovost podatkov.
- Nepreglednost sistemov, ki temeljijo na algoritmih, se lahko obravnava z zahtevami po preglednosti.
- Obstoječa pravila bo morda treba prilagoditi in pojasniti za samostojno programsko opremo, dano na trg v samostojni obliki ali naloženo na proizvod, potem ko se ta da na trg, kadar vpliva na varnost.
- Glede na vse bolj zapletene dobavne verige na področju novih tehnologij bi določbe, ki izrecno zahtevajo sodelovanje med gospodarskimi subjekti v dobavni verigi in uporabniki, lahko zagotavljale pravno varnost.

Značilnosti novih digitalnih tehnologij, kot so umetna inteligenca, internet stvari in robotika, lahko pomenijo izziv za vidike okvirov za odgovornost ter bi lahko zmanjšale njihovo učinkovitost. Nekatere izmed teh značilnosti bi lahko otežile izsledite škode nazaj do osebe, kar bi bilo v skladu z večino nacionalnih pravil nujno pri odškodninskih zahtevkih, ki temeljijo na krivdni odgovornosti. To bi lahko močno povišalo stroške za žrtve ter pomeni, da bi bilo odškodninske zahtevke zoper druge subjekte, ki niso proizvajalci, težko uveljaviti oziroma dokazati.

- Osebe, ki so utrpele škodo, povzročeno zaradi uporabe umetne inteligence, morajo uživati enako raven zaščite kot osebe, ki utrpijo škodo, ki jo povzročijo druge tehnologije, pri čemer to ne bi smelo ovirati razvoja tehnoloških inovacij.
- Vse možnosti za uresničitev tega cilja bi bilo treba previdno oceniti, vključno z možnimi spremembami direktive o odgovornosti za proizvode ter morebitno nadaljnjo usmerjeno harmonizacijo nacionalnih pravil o odgovornosti. Komisija na primer zbira mnenja, ali in v kakšni meri je morda treba ublažiti posledice kompleksnosti s prilagoditvijo dokaznega bremena, ki se zahteva v skladu z nacionalnimi pravili o odgovornosti za škodo, ki jo povzroči delovanje aplikacij umetne inteligence.

Glede na zgornjo razpravo Komisija sklepa, da bo – poleg morebitnih prilagoditev obstoječe zakonodaje – morda potrebna nova zakonodaja, ki bo posebej obravnavala umetno inteligenco, da bo pravni okvir EU primeren za trenutni in pričakovani tehnološki in komercialni razvoj.

C. PODROČJE UPORABE PRIHODNJEGA REGULATIVNEGA OKVIRA EU

Ključno vprašanje za prihodnji specifični regulativni okvir za umetno inteligenco je določitev področja njegove uporabe. Delovna predpostavka je, da bi se regulativni okvir lahko uporabljal za proizvode in storitve, ki se opirajo na umetno inteligenco. Umetno inteligenco bi bilo zato treba jasno opredeliti tako za namene te bele knjige kot za morebitne prihodnje pobude za oblikovanje politike.

Komisija je v svojem sporočilu o umetni inteligenci za Evropo zagotovila prvo opredelitev umetne inteligence[46]. Opredelitev je dodatno izpopolnila strokovna skupina na visoki ravni[47].

V vseh novih pravnih instrumentih bo morala biti opredelitev umetne inteligence dovolj prožna, da bo lahko zajela tehnični napredek, ter hkrati dovolj natančna, da bo zagotavljala potrebno pravno varnost.

Za namene te bele knjige ter za vse morebitne prihodnje razprave o pobudah politike se zdi pomembno pojasniti glavne elemente, ki sestavljajo umetno inteligenco, in sicer „podatke“ in „algoritme“. Umetno inteligenco je mogoče integrirati v strojno opremo. V primeru tehnik strojnega učenja, ki so podskupina umetne inteligence, so algoritmi naučeni, da na podlagi nabora podatkov sklepajo o določenih vzorcih in tako določijo ukrepe, ki so potrebni za dosego danega cilja. Algoritmi se lahko med uporabo še naprej učijo. Medtem ko lahko proizvodi z umetno inteligenco delujejo samostojno z zaznavanjem svojega okolja in brez vnaprej določenega sklopa navodil, pa njihovo ravnanje večinoma določijo in omejijo njihovi razvijalci. Ljudje določijo in programirajo cilj, ki bi ga moral sistem umetne inteligence optimizirati.

Pri avtonomni vožnji na primer algoritem v realnem času uporablja podatke, ki jih dobi od avtomobila (hitrost, poraba motorja, blažilniki itd.) in senzorjev, ki skenirajo celotno okolje avtomobila (cesto, znake, druga vozila, pešce itd.), da določi smer, pospešek in hitrost avtomobila, da ta pripelje na določen cilj. Algoritem na podlagi zaznanih podatkov prilagodi vožnjo razmeram na cesti in zunanjim pogojem, vključno z vedenjem drugih voznikov, da zagotovi najudobnejšo in najvarnejšo vožnjo.

EU ima strog pravni okvir, da med drugim zagotovi varstvo potrošnikov, obravnava nepoštene poslovne prakse ter varuje osebne podatke in zasebnost. Poleg tega pravni red vsebuje posebna pravila za nekatere sektorje (npr. zdravstvo, transport). Te obstoječe določbe prava EU se bodo še naprej uporabljale za umetno inteligenco, čeprav bodo morda potrebne nekatere posodobitve tega okvira, da bo odražal digitalno preobrazbo in uporabo umetne inteligence (glej oddelek B). Zato bo ta zakonodaja še naprej urejala tiste vidike, ki jih že ureja obstoječa horizontalna ali sektorska zakonodaja (npr. o medicinskih pripomočkih[48] in prometnih sistemih).

[46] COM(2018) 237 final, str. 1: „Umetna inteligenca pomeni sisteme, ki z analiziranjem svojega okolja in ukrepanjem (delno samostojnim) za doseganje posebnih ciljev kažejo inteligentno ravnanje.
Sistemi umetne inteligence lahko v celoti temeljijo na programski opremi in delujejo v virtualnem svetu (npr. glasovni pomočniki, programska oprema za analizo slik, iskalniki, sistemi za prepoznavanje govora in obraza) ali pa so vdelani v strojno opremo (npr. napredni roboti, samostojni avtomobili, brezpilotni zrakoplovi ali aplikacije za internet stvari).“

[47] Strokovna skupina na visoki ravni, Opredelitev umetne inteligence, str. 8: „Sistemi umetne inteligence so sistemi programske opreme (in po možnosti tudi strojne opreme), ki so jih oblikovali ljudje in ki, če se jim zastavi kompleksen cilj, delujejo v fizični ali digitalni razsežnosti z zaznavanjem svojega okolja prek zbiranja podatkov, interpretiranjem zbranih strukturiranih ali nestrukturiranih podatkov, sklepanjem na podlagi znanja ali obdelovanjem informacij, ki izhajajo iz teh podatkov, ter odločanjem o najboljših ukrepih za dosego zastavljenega cilja. Sistemi umetne inteligence lahko uporabljajo simbolična pravila ali se naučijo numeričnega modela, poleg tega lahko prilagodijo svoje vedenje na podlagi analize, kako so njihova prejšnja dejanja vplivala na okolje.“

[48] Na primer, varnostni vidiki in pravne posledice sistemov umetne inteligence, ki zdravnikom zagotavljajo specializirane zdravstvene informacije, sistemov umetne inteligence, ki zagotavljajo zdravstvene informacije neposredno bolnikom, in sistemov umetne inteligence, ki sami opravljajo zdravstvene posege neposredno na bolniku, se med seboj razlikujejo. Komisija preučuje te varnostne izzive in izzive glede odgovornosti, ki so značilni za zdravstvo.

Nov regulativni okvir za umetno inteligenco bi moral načeloma učinkovito dosegati zastavljene cilje, pri čemer ne sme biti preveč predpisujoč, da ne naloži nesorazmernega bremena, zlasti za MSP. Komisija meni, da bi morala za dosego takšnega ravnovesja izvajati pristop na podlagi tveganja.

Pristop na podlagi tveganja je pomemben za zagotovitev, da je regulativno posredovanje sorazmerno. Vendar pa zahteva jasna merila za razlikovanje med različnimi aplikacijami umetne inteligence, zlasti v zvezi z vprašanjem, ali so to aplikacije z visokim tveganjem ali ne[49]. Opredelitev aplikacije umetne inteligence z visokim tveganjem bi morala biti jasna in lahko razumljiva ter uporabna za vse zadevne strani. Četudi aplikacija umetne inteligence ni opredeljena kot aplikacija z visokim tveganjem, zanjo še vedno v celoti veljajo obstoječa pravila EU.

Komisija meni, da je treba dano aplikacijo umetne inteligence na splošno obravnavati kot aplikacijo z visokim tveganjem glede na to, kaj je lahko ogroženo, pri čemer se upošteva, ali tako sektor kot načrtovana uporaba vključujeta precejšnja tveganja, zlasti z vidika zaščite varnosti, pravic potrošnikov in temeljnih pravic. Natančneje, aplikacijo umetne inteligence bi bilo treba obravnavati kot aplikacijo z visokim tveganjem, kadar izpolnjuje naslednja kumulativna merila:

- Prvič, aplikacija umetne inteligence se uporablja v sektorju, v katerem je glede na značilnosti dejavnosti, ki se običajno izvajajo, mogoče pričakovati znatna tveganja. To prvo merilo zagotavlja, da je regulativno posredovanje usmerjeno na področja, na katerih so tveganja na splošno najverjetnejša. Zajeti sektorji bi morali biti posebej in izčrpno navedeni v novem regulativnem okviru. To bi bili na primer zdravstvo, promet, energija in deli javnega sektorja[50]. Seznam bi bilo treba redno pregledovati in po potrebi spremeniti glede na razvoj v praksi.

- Drugič, aplikacija umetne inteligence se v zadevnem sektorju poleg tega uporablja na tak način, da so verjetna znatna tveganja. To drugo merilo odraža potrditev, da ni nujno, da vsaka uporaba umetne inteligence v izbranih sektorjih prinaša znatna tveganja. Na primer, četudi je zdravstvo na splošno pomemben sektor, napaka v sistemu naročanja bolnikov v bolnišnici običajno ne predstavlja tako visokega tveganja, da bi to upravičevalo zakonodajno posredovanje. Ocena stopnje tveganja dane uporabe bi lahko temeljila na posledicah za prizadete strani. Na primer, uporabe aplikacij umetne inteligence, ki imajo pravne ali podobno pomembne posledice za pravice posameznika ali podjetje, predstavljajo tveganje poškodbe, smrti ali znatne premoženjske ali nepremoženjske škode ali imajo posledice, ki se jim posamezniki ali pravne osebe ne morejo razumno izogniti.

Uporaba dveh kumulativnih meril bi zagotovila, da je področje uporabe regulativnega okvira ciljno usmerjeno in zagotavlja pravno varnost. Obvezne zahteve iz novega regulativnega okvira za umetno inteligenco (glej oddelek D spodaj) bi se načeloma uporabljale le za tiste aplikacije, ki so v skladu s tema kumulativnima meriloma opredeljene kot aplikacije z visokim tveganjem.

Ne glede na navedeno so možni tudi izjemni primeri, ko se zaradi prisotnega tveganja uporaba aplikacij umetne inteligence za določene namene šteje za aplikacijo z visokim tveganjem sama po sebi – tj. neodvisno od zadevnega sektorja in ali bi se še uporabljale spodaj navedene zahteve[51]. Kot primer je možno zlasti naslednje:

[49] V zakonodaji EU so tveganja lahko kategorizirana drugače, kot je opisano tukaj, odvisno od področja, kot je na primer varnost proizvodov.

[50] Javni sektor bi lahko vključeval področja, kot so azil, migracije, nadzor meje in pravosodje, socialna varnost ter službe za zaposlovanje.

[51] Pomembno je poudariti, da se morda uporabljajo tudi drugi deli zakonodaje EU. Na primer, za varnost aplikacije umetne inteligence, integrirane v potrošniški proizvod, se lahko uporablja direktiva o splošni varnosti proizvodov.

- Glede na pomen za posameznike in glede na pravni red EU, ki obravnava enakost pri zaposlovanju, bi se uporaba aplikacij umetne inteligence za postopke zaposlovanja ter v razmerah, ki vplivajo na pravice delavcev, vedno štela za aplikacijo z visokim tveganjem, zato bi bilo treba v vsakem primeru uporabljati spodaj navedene zahteve. Razmisliti bi bilo treba tudi o drugih specifičnih uporabah aplikacij, ki vplivajo na pravice potrošnikov.

- Uporaba aplikacij umetne inteligence za biometrično identifikacijo na daljavo [52] in drugih vsiljivih tehnologij za nadzor se bo vedno štela za aplikacijo z visokim tveganjem in zato bi se spodaj navedene zahteve vedno uporabljale.

D. VRSTE ZAHTEV

Pri oblikovanju prihodnjega regulativnega okvira za umetno inteligenco bo treba določiti vrste obveznih pravnih zahtev, ki jih je treba uvesti za zadevne akterje. Te zahteve se lahko podrobneje opredelijo v standardih. Kot je navedeno v oddelku C zgoraj in kot dodatek že obstoječi zakonodaji, bi se navedene zahteve uporabljale le za aplikacije umetne inteligence z visokim tveganjem, s čimer bi se zagotovilo, da je vsako regulativno posredovanje usmerjeno in sorazmerno.

Ob upoštevanju smernic strokovne skupine na visoki ravni in zgornjih navedb bi lahko zahteve za aplikacije umetne inteligence z visokim tveganjem vključevale naslednje ključne značilnosti, ki so podrobneje obravnavane v pododdelkih v nadaljevanju:

- učni podatki;
- hramba podatkov in evidenc;
- informacije, ki jih je treba zagotoviti;
- robustnost in natančnost;
- človeški nadzor;
- posebne zahteve za nekatere posebne aplikacije umetne inteligence, kot so tiste, ki se uporabljajo za biometrično identifikacijo na daljavo.

Za zagotovitev pravne varnosti bodo te zahteve nadalje opredeljene, da se zagotovi jasno referenčno merilo za vse akterje, ki jih morajo izpolnjevati.

a) Učni podatki

Bolj kot kdaj koli je pomembno spodbujati, krepiti in braniti vrednote in pravila EU ter zlasti pravice državljank in državljanov, ki izhajajo iz prava EU. Ta prizadevanja nedvomno zajemajo tudi aplikacije umetne inteligence z visokim tveganjem, ki se tržijo in uporabljajo v EU.

Kot je bilo povedano prej – brez podatkov ni umetne inteligence. Delovanje številnih sistemov umetne inteligence ter dejanja in odločitve, ki jih lahko izvedejo oziroma sprejmejo, so v veliki meri odvisni od nabora podatkov, iz katerih so se sistemi učili. Zato bi bilo treba sprejeti potrebne ukrepe za zagotovitev, da so podatki, ki se uporabljajo za učenje sistemov umetne inteligence, skladni z vrednotami in pravili EU, zlasti v zvezi z varnostjo in obstoječimi zakonodajnimi pravili za varstvo

[52] Biometrična identifikacija na daljavo bi se morala razlikovati od biometrične avtentikacije (slednja je varnostni postopek, ki se opira na edinstvene biološke značilnosti posameznika, da se preveri, ali je oseba, za katero trdi, da je). Pri biometrični identifikaciji na daljavo se identitete več oseb ugotavljajo na daljavo, in sicer s pomočjo biometričnih identifikatorjev (prstni odtisi, podoba obraza, šarenica, žilni vzorci itd.), v javnem prostoru in neprekinjeno, tako da se primerjajo s podatki, shranjenimi v zbirkah podatkov.

temeljnih pravic. Za nabor podatkov, ki se uporabljajo za učenje sistemov umetne inteligence, lahko veljajo naslednje zahteve:

- Zahteve, ki zagotavljajo razumna zagotovila, da je poznejša uporaba proizvodov ali storitev, ki temeljijo na sistemih umetne inteligence, varna, ker izpolnjuje standarde, določene v veljavnih varnostnih predpisih EU (obstoječih in morebitnih dopolnilnih). To so na primer zahteve, ki zagotavljajo, da se sistemi umetne inteligence učijo iz nabora podatkov, ki je dovolj širok in zajema vse relevantne scenarije, ki so potrebni za izognitev nevarnim situacijam.

- Zahteve za sprejetje razumnih ukrepov za zagotovitev, da poznejša uporaba sistemov umetne inteligence ne da rezultatov, ki povzročajo prepovedano diskriminacijo. Te zahteve bi lahko vključevale zlasti obveznosti za uporabo naborov podatkov, ki so dovolj reprezentativni, zlasti za zagotovitev, da so v podatkih v teh naborih ustrezno zastopani ustrezni vidiki spola, etnične pripadnosti in druge možne podlage za prepovedano diskriminacijo.

- Zahteve, katerih namen je zagotoviti ustrezno varstvo zasebnosti in osebnih podatkov med uporabo umetnointeligenčno omogočenih proizvodov in storitev. Splošna uredba o varstvu podatkov in direktiva o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj urejata ta vprašanja, če spadajo na njuna področja uporabe.

b) Hramba evidenc in podatkov

Ob upoštevanju elementov, kot sta kompleksnost in nepreglednost številnih sistemov umetne inteligence, ter s tem povezanih težav, ki lahko ovirajo učinkovito preverjanje skladnosti z veljavnimi pravili ter njihovo izvrševanje, so potrebne zahteve glede hrambe evidenc v zvezi s programiranjem algoritma, podatkov, ki se uporabljajo za učenje sistemov umetne inteligence z visokim tveganjem, in v nekaterih primerih glede hrambe podatkov samih. Te zahteve v bistvu omogočajo sledenje in preverjanje potencialno problematičnih dejanj ali odločitev sistemov umetne inteligence. To bi moralo ne le olajšati nadzor in izvrševanje, ampak tudi povečati spodbude za zadevne gospodarske subjekte, da že vse od začetka upoštevajo potrebo po spoštovanju teh pravil.

V ta namen bi regulativni okvir lahko določal, da je treba hraniti naslednje:

- točne evidence o naboru podatkov, ki so se uporabili za učenje in preskušanje sistemov umetne inteligence, vključno z opisom glavnih značilnosti in potekom izbora nabora podatkov;

- v nekaterih upravičenih primerih tudi sam nabor podatkov;

- dokumentacijo o metodologijah, postopkih in tehnikah programiranja[53] in učenja, uporabljenih za izgradnjo, preskušanje in potrjevanje sistemov umetne inteligence, vključno, kadar je potrebno, dokumentacijo v zvezi z varnostjo in izogibanjem pristranskosti, ki bi lahko privedla do prepovedane diskriminacije.

Evidence, dokumentacijo in po potrebi nabore podatkov bi bilo treba hraniti za omejeno in razumno dolgo obdobje, da se zagotovi učinkovito izvrševanje zadevne zakonodaje. Sprejeti bi bilo treba ukrepe za zagotovitev, da so na voljo na zahtevo, zlasti za preskušanje ali inšpekcijski pregled, ki ga

[53] Na primer, dokumentacijo o algoritmu, vključno s tem, kaj model optimizira, katere uteži so na začetku pripisane določenim parametrom itd.

izvaja pristojni organi. Po potrebi se sprejmejo ureditve, s katerimi se zagotovi varovanje zaupnih informacij, kot so poslovne skrivnosti.

c) Obveščanje

Preglednost se ne zahteva zgolj glede zahtev o hrambi evidenc, navedenih v točki c) zgoraj, ampak tudi širše. Za doseganje zastavljenih ciljev – zlasti za spodbujanje odgovorne uporabe umetne inteligence, vzpostavljanje zaupanja in lažjo uporabo pravnih sredstev, kjer je to potrebno – je pomembno, da se na proaktiven način zagotovijo ustrezne informacije o uporabi sistemov umetne inteligence z visokim tveganjem.

V skladu s tem bi se lahko preučile naslednje zahteve:

- Zagotavljanje jasnih informacij glede zmogljivosti in omejitev sistemov umetne inteligence, zlasti čemu so sistemi namenjeni, pogojev, pod katerimi se lahko pričakuje, da bodo delovali, kot je bilo predvideno, in pričakovane ravni natančnosti pri doseganju določenega namena. Te informacije so pomembne zlasti za uvajalce sistemov, lahko pa so pomembne tudi za pristojne organe in prizadete strani.

- Državljani bi morali biti jasno obveščeni, kdaj imajo stik s sistemom umetne inteligence in ne s človekom. Čeprav zakonodaja EU o varstvu podatkov že vsebuje nekatera tovrstna pravila[54], se lahko zahtevajo dodatne zahteve za doseganje zgoraj navedenih ciljev. V tem primeru bi se bilo treba izogniti nepotrebnim bremenom. Zato takih informacij ni treba zagotoviti, na primer v primerih, ko je državljankam in državljanom takoj očitno, da imajo stik s sistemi umetne inteligence. Poleg tega je pomembno, da so predložene informacije objektivne, jedrnate in lahko razumljive. Način zagotavljanja informacij bi moral biti prilagojen posebnim okoliščinam.

d) Robustnost in natančnost

Sistemi umetne inteligence – in zlasti aplikacije umetne inteligence z visokim tveganjem – morajo biti tehnično robustni in točni, da bi bili zanesljivi. To pomeni, da je take sisteme treba razviti na odgovoren način in s predhodno ustrezno obravnavo tveganj, ki jih lahko ustvarijo. Njihov razvoj in delovanje morata zagotavljati, da sistemi umetne inteligence delujejo zanesljivo, kot je bilo predvideno. Treba je sprejeti vse razumne ukrepe, da se čim bolj zmanjša tveganje nastanka škode.

V skladu s tem se lahko upoštevajo naslednji elementi:

- zahteve, ki zagotavljajo, da so sistemi umetne inteligence robustni in točni ali vsaj pravilno odražajo njihovo raven točnosti v vseh fazah življenjskega cikla;

- zahteve, ki zagotavljajo, da so rezultati ponovljivi;

- zahteve, ki zagotavljajo, da lahko sistemi umetne inteligence ustrezno obravnavajo napake ali neskladnosti v vseh fazah življenjskega cikla;

[54] V skladu s členom 13(2)(f) splošne uredbe o varstvu podatkov morajo upravljavci pri pridobivanju osebnih podatkov posameznikom, na katere se podatki nanašajo, zagotoviti dodatne informacije, ki so potrebne za zagotovitev poštene in pregledne obdelave, o obstoju avtomatiziranega sprejemanja odločitev ter nekatere dodatne informacije.

- zahteve, ki zagotavljajo, da so sistemi umetne inteligence odporni tako proti očitnim napadom kot proti bolj prefinjenim napadom z namenom manipulacije podatkov ali samih algoritmov ter da se v takih primerih sprejmejo blažilni ukrepi.

e) Človeški nadzor

Človeški nadzor pomaga zagotavljati, da sistem umetne inteligence ne ogroža človekove avtonomije ali nima drugih škodljivih učinkov. Cilj zaupanja vredne, etične in na humanocentrične umetne inteligence je mogoče doseči le z zagotavljanjem ustrezne vloge ljudi pri aplikacijah umetne inteligence z visokim tveganjem.

Čeprav se aplikacije umetne inteligence, obravnavane v tej beli knjigi, za posebno pravno ureditev vse štejejo za aplikacije z visokim tveganjem, se lahko primerna oblika in stopnja človeškega nadzora razlikuje med posameznimi primeri. Nadzor je odvisen zlasti od nameravane uporabe sistemov in posledic, ki bi jih uporaba lahko imela za prizadete državljanke in državljane in pravne osebe. Prav tako ne posega v pravne pravice, določene s splošno uredbo o varstvu podatkov, kadar sistem umetne inteligence obdeluje osebne podatke. Človeški nadzor bi se lahko na primer, med drugim, izvajal na naslednje načine:

- rezultat dela sistema umetne inteligence se ne uporabi, razen če ga človek predhodno ne pregleda in potrdi (npr. vlogo za socialnovarstveni prejemek lahko zavrne samo človek);

- rezultat dela sistema umetne inteligence se uporabi takoj, vendar se naknadno izvede človeško posredovanje (npr. zavrnitev vloge za kreditno kartico se lahko obdela s sistemom umetne inteligence, vendar mora biti pozneje možen človeški pregled);

- spremljanje sistema umetne inteligence med delovanjem ter možnost posredovanja v realnem času in deaktiviranja sistema (npr. v avtomobilu brez voznika je na voljo gumb „stop“ ali postopek za primer, če človek ugotovi, da avtomobil ne deluje varno);

- v fazi oblikovanja z uvedbo omejitev delovanja v sisteme umetne inteligence (npr. avtomobil brez voznika preneha delati v določenih pogojih nizke vidljivosti, ko lahko senzorji postanejo manj zanesljivi, ali v kakršnih koli razmerah ohranja določeno razdaljo od prejšnjega vozila).

f) Posebne zahteve za biometrično identifikacijo na daljavo

Zbiranje in uporaba biometričnih podatkov[55] za identifikacijo na daljavo[56], na primer z uporabo prepoznavanja obrazov na javnih mestih, prinaša specifična tveganja za temeljne pravice[57]. Posledice,

[55] Biometrični podatki so opredeljeni kot osebni podatki, „ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki.“ (Člen 3(13) direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, člen 4(14) splošne uredbe o varstvu podatkov in člen 3(18) Uredbe (EU) 2018/1725).)

[56] V zvezi s prepoznavanjem obrazov identifikacija pomeni, da se predloga s podobo obraza osebe primerja s številnimi drugimi predlogami, shranjenimi v zbirki podatkov, da se ugotovi, ali je podoba osebe tam shranjena. Avtentikacija (ali preverjanje) na drugi strani pa pogosto pomeni ujemanje med dvema predlogama. Omogoča primerjavo dveh biometričnih predlog, za kateri se navadno domneva, da pripadata istemu posamezniku. Dve biometrični predlogi se primerjata, da se ugotovi, ali je oseba na obeh podobah ista.

Tak postopek na primer izvajajo avtomatizirani sistemi mejnega nadzora (ABC), ki se uporabljajo za mejno kontrolo na letališčih.

[57] Na primer za dostojanstvo ljudi. V povezavi s tem so pravice do spoštovanja zasebnega življenja in varstva osebnih podatkov v središču pomislekov glede spoštovanja temeljnih pravic pri uporabi tehnologije za prepoznavanje obrazov.

ki jih ima uporaba sistemov umetne inteligence za biometrično identifikacijo na daljavo na temeljne pravice, se lahko precej razlikujejo glede na namen, okoliščine in področje uporabe.

Pravila EU o varstvu podatkov načeloma prepovedujejo obdelavo biometričnih podatkov za namene edinstvene identifikacije fizične osebe, razen pod posebnimi pogoji[58]. In sicer, v skladu s splošno uredbo o varstvu podatkov se lahko taka obdelava izvede le iz omejenega števila razlogov, pri čemer je glavni razlog bistveni javni interes. V tem primeru mora obdelava potekati v skladu s pravom EU ali nacionalnim pravom, ob upoštevanju zahtev glede sorazmernosti, spoštovanju bistva pravice do varstva podatkov in ustreznih zaščitnih ukrepov. V skladu z direktivo o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj mora biti takšna obdelava nujno potrebna in so zanjo potrebni dovoljenje v skladu s pravom EU ali nacionalnim pravom ter ustrezni zaščitni ukrepi. Ker bi vsakršna obdelava biometričnih podatkov za namene edinstvene identifikacije fizične osebe pomenila izjemo od prepovedi iz prava EU, bi se zanjo uporabljala Listina EU o temeljnih pravicah.

Iz tega sledi, da se lahko umetna inteligenca v skladu z veljavnimi pravili EU o varstvu podatkov in Listino o temeljnih pravicah uporablja le za biometrično identifikacijo na daljavo, kadar je taka uporaba ustrezno utemeljena, sorazmerna in se zanjo uporabljajo ustrezni zaščitni ukrepi.

Da bi obravnavala morebitne družbene pomisleke v zvezi z uporabo umetne inteligence v take namene na javnih mestih in preprečila razdrobljenost notranjega trga, bo Komisija začela široko evropsko razpravo o morebitnih posebnih okoliščinah, ki bi lahko upravičile takšno uporabo, ter o skupnih zaščitnih ukrepih.

E. NASLOVNIKI

V zvezi z naslovniki pravnih zahtev, ki bi veljale v zvezi z zgoraj navedenimi aplikacijami umetne inteligence z visokim tveganjem, je treba upoštevati dve glavni vprašanji.

Prvič, odpira se vprašanje razdelitve obveznosti med zadevnimi gospodarskimi subjekti. Številni akterji so vključeni v življenjski cikel sistema umetne inteligence. Mednje spadajo razvijalec, uvajalec (oseba, ki uporablja proizvod ali storitev, podprta z umetno inteligenco) in morda drugi (proizvajalec, distributer ali uvoznik, ponudnik storitev, poklicni ali zasebni uporabnik).

Komisija meni, da bi bilo treba v prihodnjem regulativnem okviru vsako obveznost nasloviti na akterje, ki so najprimernejši za obravnavanje morebitnih tveganj. Na primer, medtem ko so razvijalci umetne inteligence v najboljšem položaju za obravnavo tveganj, ki se pojavijo med razvojem, pa je njihova zmožnost za nadzor tveganj med uporabo bolj omejena. V tem primeru bi morala za uvajalca veljati ustrezna obveznost. To ne vpliva na vprašanje, katera stran je odgovorna za škodo, ki jo utrpijo končni uporabniki ali druge stranke in katerim je treba zagotoviti učinkovit dostop do sodnega varstva. V skladu z zakonodajo EU o odgovornosti za proizvode se odgovornost za proizvode z napako pripiše proizvajalcu, in sicer brez poseganja v nacionalno zakonodajo, ki lahko dopušča tudi izterjavo od drugih strank.

Drugič, obstaja vprašanje glede geografskega področja uporabe zakonodajnega posredovanja. Komisija meni, da je bistvenega pomena, da zahteve veljajo za vse zadevne gospodarske subjekte, ki v

---

Možen je tudi vpliv na nediskriminacijo in pravice posebnih skupin, kot so otroci, starejši in invalidi. Poleg tega uporaba tehnologije ne sme ogroziti svobode izražanja, združevanja in zbiranja. Glej: Facial recognition technology: fundamental rights considerations in the context of law enforcement (Tehnologija prepoznavanja obrazov: spoštovanje temeljnih pravic pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj), https://fra.europa.eu/en/publication/2019/facial-recognition.

[58] Člen 9 splošne uredbe o varstvu podatkov in člen 10 direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj. Glej tudi člen 10 Uredbe (EU) 2018/1725 (uporablja se za institucije in organe EU).

EU zagotavljajo umetnointeligenčno omogočene proizvode ali storitve, ne glede na to, ali imajo sedež v EU ali ne. V nasprotnem primeru zgoraj omenjenih ciljev zakonodajnega posredovanja ne bi bilo mogoče v celoti doseči.

F. SKLADNOST IN IZVRŠEVANJE

Za zagotovitev, da je umetna inteligenca vredna zaupanja, varna in spoštuje evropske vrednote in pravila, je treba v praksi spoštovati veljavne pravne zahteve, ki jih morajo učinkovito upoštevati tako pristojni nacionalni in evropski organi kot tudi prizadete strani. Pristojni organi bi morali imeti možnost, da opravijo preiskavo posameznih primerov ter tudi ocenijo vpliv na družbo.

Glede na visoko tveganje, ki ga nekatere aplikacije umetne inteligence predstavljajo za državljanke in državljane ter našo družbo (glej oddelek A zgoraj), Komisija na tej stopnji meni, da bi bilo potrebno predhodno ugotavljanje skladnosti, da se preveri in zagotovi upoštevanje nekaterih zgoraj navedenih obveznih zahtev, ki veljajo za aplikacije z visokim tveganjem (glej oddelek D zgoraj). Predhodno ugotavljanje skladnosti lahko vključuje postopke za preskušanje, inšpekcijski pregled ali certificiranje[59]. Lahko vključuje preverjanja algoritmov in naborov podatkov, ki se uporabljajo v razvojni fazi.

Ugotavljanje skladnosti za aplikacije umetne inteligence z visokim tveganjem bi moralo biti del mehanizmov za ugotavljanje skladnosti, ki že obstajajo za številne proizvode, ki se dajejo na notranji trg EU. Kadar se na takšne že obstoječe mehanizme ni mogoče zanašati, bo morda treba vzpostaviti podobne mehanizme, pri tem pa se opirati na najboljšo prakso in morebiten prispevek zainteresiranih strani in evropskih organizacij za standardizacijo. Vsak takšen nov mehanizem bi moral biti sorazmeren in nediskriminatoren ter bi moral uporabljati pregledna in objektivna merila v skladu z mednarodnimi obveznostmi.

Pri oblikovanju in izvajanju sistema, ki se opira na predhodno ugotavljanje skladnosti, je treba upoštevati zlasti naslednje:

- Vse zgoraj navedene zahteve morda niso primerne za preverjanje s predhodnim ugotavljanjem skladnosti. Tako na primer zahteva glede informacij, ki jih je treba zagotoviti, običajno ni primerna za preverjanje s takšnim ugotavljanjem.

- Zlasti je treba upoštevati možnost, da se nekateri sistemi umetne inteligence razvijajo in se učijo iz izkušenj, zaradi česar je ugotavljanje skladnosti morda treba ponavljati tekom življenjske dobe zadevnih sistemov umetne inteligence.

- Potreba po preverjanju podatke, ki se uporabljajo za učenje, ter zadevne metodologije, postopke in tehnike programiranja in učenja za izgradnjo, preskušanje in potrjevanje sistemov umetne inteligence.

- Če ugotavljanje skladnosti pokaže, da sistem umetne inteligence ne izpolnjuje zahtev, na primer v zvezi s podatki, ki se uporabljajo za njegovo učenje, je treba ugotovljene pomanjkljivosti odpraviti, na primer s ponovnim učenjem sistema v EU na tak način, da so izpolnjene vse veljavne zahteve.

[59] Sistem bi temeljil na postopkih ugotavljanja skladnosti v EU, glej Sklep 768/2008/ES ali Uredbo (EU) 2019/881 (uredba o kibernetski varnosti), upošteval pa bi posebnosti umetne inteligence. Glej Modri vodnik za izvajanje predpisov EU o proizvodih iz leta 2014.

Ugotavljanje skladnosti bi bilo obvezno za vse gospodarske subjekte, za katere zahteve veljajo, ne glede na njihov sedež[60]. Da bi se omejilo breme za MSP, se lahko predvidi nekaj podpornih struktur, tudi prek vozlišč za digitalne inovacije. Poleg tega bi lahko izpolnjevanje zahtev olajšali standardi in namenska spletna orodja.

Vsako predhodno ugotavljanje skladnosti ne bi smelo posegati v spremljanje spoštovanja predpisov in naknadno izvrševanje, ki ju izvajajo pristojni nacionalni organi. To velja za aplikacije umetne inteligence z visokim tveganjem, pa tudi za druge aplikacije umetne inteligence, za katere veljajo pravne zahteve, čeprav so nacionalni pristojni organi zaradi velikega tveganja, povezanega s prvimi aplikacijami, morda posebej pozorni na te. Naknadne kontrole bi morala omogočati ustrezna dokumentacija o zadevnih aplikacijah umetne inteligence (glej oddelek E zgoraj) ter po potrebi možnost, da tretje strani, kot so pristojni organi, preskusijo takšne aplikacije. To je lahko zlasti pomembno, kadar se pojavijo tveganja glede temeljnih pravic, ki so odvisna od okoliščin. Takšno spremljanje skladnosti z zakonodajo bi moralo biti del sistema stalnega nadzora trga. Vidiki, povezani z upravljanjem, so nadalje obravnavani v oddelku H spodaj.

Poleg tega bi bilo treba tako za aplikacije umetne inteligence z visokim tveganjem kot za druge aplikacije umetne inteligence zagotoviti učinkovito pravno sredstvo za stranke, za katere imajo sistemi umetne inteligence negativne posledice. Vprašanja v zvezi z odgovornostjo so nadalje obravnavana v poročilu o okviru za varnost in odgovornost, ki je priložen tej beli knjigi.

G. PROSTOVOLJNO OZNAČEVANJE APLIKACIJ UMETNE INTELIGENCE BREZ VISOKEGA TVEGANJA

Za aplikacije umetne inteligence, ki se ne štejejo za aplikacije z visokim tveganjem (glej oddelek C zgoraj) in zato zanje ne veljajo obvezne zahteve, obravnavane zgoraj (glej oddelke D, E in F zgoraj), bi bilo možno poleg veljavne zakonodaje uvesti shemo prostovoljnega označevanja.

V okviru te sheme bi se lahko zainteresirani gospodarski subjekti, za katere obvezne zahteve ne veljajo, odločili, da prostovoljno sprejmejo bodisi te zahteve bodisi poseben sklop podobnih zahtev, ki bi bile določene posebej za namene prostovoljne sheme. Zadevni gospodarski subjekti bi nato za svoje aplikacije umetne inteligence prejeli znak kakovosti.

Zadevni gospodarski subjekti bi s tem znakom o prostovoljni skladnosti pokazali, da so njihovi umetnointeligenčno omogočeni proizvodi in storitve zanesljivi. Tako bi se uporabnikom omogočilo, da enostavno prepoznajo, da so zadevni proizvodi in storitve v skladu z nekaterimi objektivnimi in standardiziranimi referenčnimi vrednostmi na ravni EU, ki presegajo običajno veljavne pravne obveznosti. To bi pomagalo izboljšati zaupanje uporabnikov v sisteme umetne inteligence in spodbujati splošno uvajanje tehnologije.

Ta možnost bi pomenila oblikovanje novega pravnega instrumenta, ki bi določal okvir za prostovoljno označevanje za razvijalce in/ali uvajalce sistemov umetne inteligence, ki se ne štejejo za aplikacije z visokim tveganjem. Medtem ko bi bila udeležba v shemi označevanja prostovoljna, pa bi postalo izpolnjevanje zahtev zavezujoče za razvijalca ali uvajalca, ko bi se odločil za uporabo oznake. Kombinacija predhodnega in naknadnega izvrševanja bi morala zagotoviti, da so vse zahteve izpolnjene.

H. UPRAVLJANJE

[60] Kar zadeva ustrezno strukturo upravljanja, vključno z organi, imenovanimi za izvajanje ugotavljanj skladnosti, glej oddelek H spodaj.

Evropska struktura upravljanja umetne inteligence v obliki okvira za sodelovanje pristojnih nacionalnih organov je potrebna, da bi se izognili razdrobljenosti odgovornosti, povečali zmogljivosti v državah članicah in zagotovili, da se Evropa sama postopoma opremi z zmogljivostmi, ki so potrebne za preskušanje in certificiranje umetnointeligenčno omogočenih proizvodov in storitev. V tem kontekstu bi bilo koristno podpreti pristojne nacionalne organe, da se jim omogoči, da izpolnjujejo svoje naloge na področjih, kjer se umetna inteligenca uporablja.

Evropska struktura upravljanja bi lahko imela različne naloge, kot so forum za redno izmenjavo informacij in najboljših praks, prepoznavanje nastajajočih trendov, svetovanje o dejavnostih standardizacije in certificiranje. Prav tako bi morala imeti ključno vlogo pri lajšanju izvajanja pravnega okvira, na primer z izdajanjem smernic in mnenj ter zagotavljanjem strokovnega znanja. V ta namen bi se morala opreti na mrežo nacionalnih organov ter na sektorske mreže in regulativne organe tako na nacionalni ravni kot na ravni EU. Poleg tega bi Komisiji lahko pomagal odbor strokovnjakov.

Struktura upravljanja bi morala jamčiti največje možno sodelovanje zainteresiranih strani. Z zainteresiranimi stranmi – organizacijami potrošnikov in socialnimi partnerji, podjetji, raziskovalci in organizacijami civilne družbe – bi se bilo treba posvetovati o izvajanju in nadaljnjem razvoju okvira.

Glede na že obstoječe strukture na področjih, kot so finance, farmacevtski izdelki, letalstvo, medicinski pripomočki, varstvo potrošnikov in varstvo podatkov, predlagana struktura upravljanja ne bi smela podvajati obstoječih funkcij. Namesto tega bi morala vzpostaviti tesne stike z drugimi pristojnimi organi EU in nacionalnimi pristojnimi organi iz različnih sektorjev, da bi dopolnila obstoječe strokovno znanje in pomagala obstoječim organom pri spremljanju in nadzoru dejavnosti gospodarskih subjektov, ki vključujejo umetnointeligenčno omogočene proizvode in storitve.

Nazadnje, če se izbere ta možnost, se lahko izvajanje ugotavljanja skladnosti zaupa priglašenim organom, ki jih določijo države članice. Centri za preskušanje bi morali omogočati neodvisno revizijo in oceno sistemov umetne inteligence v skladu z zgoraj navedenimi zahtevami. Neodvisno ugotavljanje bo povečalo zaupanje in zagotovilo nepristranskost. Prav tako bi lahko olajšala delo ustreznih pristojnih organov.

EU ima odlične centre za preskušanje in ocenjevanje ter bi morala razviti svoje zmogljivosti tudi na področju umetne inteligence. Gospodarski subjekti s sedežem v tretjih državah, ki želijo vstopiti na notranji trg, bi za takšno oceno lahko zaprosili imenovane organe s sedežem v EU ali imenovane organe tretjih držav, če je z zadevnimi tretjimi državami sklenjen sporazum o vzajemnem priznavanju.

Struktura upravljanja v zvezi z umetno inteligenco in morebitno ugotavljanje skladnosti, o katerih je tukaj govora, ne bi spreminjala pooblastil in odgovornosti, ki jih obstoječa zakonodaja EU nalaga zadevnim pristojnim organom v specifičnih sektorjih ali glede specifičnih vprašanj (finance, farmacevtski izdelki, letalstvo, medicinski pripomočki, varstvo potrošnikov, varstvo podatkov ind.).

6. ZAKLJUČEK

Umetna inteligenca je strateška tehnologija, ki državljankam in državljanom, podjetjem in družbi kot celoti zagotavlja številne koristi, pod pogojem, da je humanocentrična, etična, trajnostna in spoštuje temeljne pravice in vrednote. Umetna inteligenca pomembno izboljšuje učinkovitost in produktivnost, kar lahko okrepi konkurenčnost evropske industrije in izboljša blaginjo državljank in državljanov. Prav tako lahko prispeva k iskanju rešitev za nekatere najbolj pereče družbene izzive, vključno z bojem proti podnebnim spremembam in degradaciji okolja, izzive, povezane s trajnostnostjo in demografskimi spremembami ter zaščito naših demokracij in, kjer je to potrebno in sorazmerno, bojem proti kriminalu.

Evropa mora, da bi v celoti izkoristila priložnosti, ki jih ponuja umetna inteligenca, razviti in okrepiti potrebne industrijske in tehnološke zmogljivosti. Kot je določeno v priloženi evropski strategiji za podatke, so potrebni tudi ukrepi, ki bodo EU omogočili, da postane svetovno vozlišče za podatke.

Cilj evropskega pristopa k umetni inteligenci je spodbujati inovacijske zmogljivosti Evrope na področju umetne inteligence, hkrati pa podpirati razvoj in uvajanje etične in zaupanja vredne umetne inteligence v vse sektorje gospodarstva EU. Umetna inteligenca mora delati za ljudi in biti sila za dobro v družbi.

Komisija s to belo knjigo in priloženim poročilom o okviru za varnost in odgovornost začenja obsežno posvetovanje z državami članicami, civilno družbo, industrijo in akademiki akademskimi krogi o konkretnih predlogih za evropski pristop k umetni inteligenci. Ti vključujejo tako ukrepe politike za spodbujanje naložb v raziskave in inovacije, krepitev razvoja znanj in spretnosti ter podporo uvajanju umetne inteligence v MSP, kot tudi predloge za ključne elemente prihodnjega regulativnega okvira. To posvetovanje bo omogočilo celovit dialog z vsemi zadevnimi stranmi, Komisija pa bo povratne informacije uporabila v svojih nadaljnjih ukrepih.

Komisija poziva k predložitvi pripomb o predlogih iz bele knjige v okviru odprtega javnega posvetovanja, ki je dostopno na strani https://ec.europa.eu/info/consultations_sl. Posvetovanje je odprto za mnenja do 19. maja 2020.

Komisija običajno objavlja prispevke, prejete v okviru javnega posvetovanja. Vendar pa je mogoče zaprositi, da prispevki ali njihovi deli ostanejo zaupni. V tem primeru vas prosimo, da na naslovni strani vašega prispevka jasno navedete, da ne želite javne objave, Komisiji pa pošljite tudi nezaupno različico vašega prispevka za objavo.