EUROPSKA
KOMISIJA

Bruxelles, 19.2.2020.
COM(2020) 65 final

BIJELA KNJIGA

o umjetnoj inteligenciji – Europski pristup izvrsnosti i izgradnji povjerenja

Bijela knjiga o umjetnoj inteligenciji
Europski pristup izvrsnosti i izgradnji povjerenja

Umjetna inteligencija (UI) brzo se razvija. Promijenit će naše živote jer će poboljšati zdravstvenu skrb (npr. omogućit će preciznije dijagnoze i bolju prevenciju bolesti), povećati učinkovitost poljoprivrede, pridonijeti ublažavanju klimatskih promjena i prilagodbi tim promjenama, povećati učinkovitost proizvodnih sustava zahvaljujući prediktivnom održavanju i unaprijediti sigurnost Europljana. Mnoge druge načine na koje će UI utjecati na nas još ne možemo niti zamisliti. Jednako tako, umjetnu inteligenciju prati niz potencijalnih rizika, kao što su netransparentno donošenje odluka, rodno uvjetovana ili druga vrsta diskriminacije, zadiranje u privatni život ili upotreba u kriminalne svrhe.

Zbog oštre globalne konkurencije treba nam solidan europski pristup koji se temelji na europskoj strategiji za umjetnu inteligenciju predstavljenoj u travnju 2018.[1] Kako bi iskoristio prilike i suočio se s izazovima koje donosi umjetna inteligencija, EU mora djelovati kao cjelina i definirati vlastiti način na koji želi promicati razvoj i primjenu UI-ja te ga utemeljiti na europskim vrijednostima.

Komisija predano radi na omogućivanju znanstvenog napretka, očuvanju tehnološkog vodstva EU-a i stavljanju novih tehnologija u službu svih Europljana, poboljšavajući im tako živote uz poštovanje njihovih prava.

Predsjednica Komisije Ursula von der Leyen u svojim je političkim smjernicama [2] najavila koordinirani europski pristup etičkim implikacijama umjetne inteligencije i njezinim posljedicama na ljude te promišljanje o boljem iskorištavanju velikih količina podataka za uvođenje inovacija.

Komisija se stoga zauzima za regulatorni pristup usmjeren na ulaganja s dvojakim ciljem: uvođenje umjetne inteligencije i suzbijanje rizika povezanih s određenim načinima upotrebe te nove tehnologije. Svrha je ove Bijele knjige iznijeti političke opcije za postizanje tih ciljeva. U njoj se ne razmatraju razvoj i upotreba UI-ja u vojne svrhe. Komisija poziva države članice, druge europske institucije i sve dionike, uključujući industriju, socijalne partnere, organizacije civilnog društva, znanstvenike, širu javnost i sve zainteresirane strane, da reagiraju na opcije iznesene u nastavku i tako pridonesu odlukama koje će Komisija ubuduće donositi u tom području.

1. UVOD

Budući da digitalna tehnologija postaje sve važniji dio svakog aspekta života ljudi, oni bi u nju trebali imati povjerenja. Preduvjet za uvođenje takve tehnologije je i pouzdanost. Upravo u pouzdanosti leži prilika za Europu, koja je odana vrijednostima i vladavini prava te dokazano sposobna stvarati sigurne, pouzdane i sofisticirane proizvode i usluge u najrazličitijim područjima, kao što su aeronautika, energetika, automobilska industrija i proizvodnja medicinske opreme.

Sadašnji i budući održivi gospodarski rast i društvena dobrobit Europe sve se više oslanjaju na vrijednost koja proizlazi iz podataka. Umjetna inteligencija jedno je od najvažnijih područja za podatkovno gospodarstvo. Danas je većina podataka povezana s potrošačima te se pohranjuje i obrađuje na središnjoj infrastrukturi u oblaku. S druge strane, mnogo opsežniji budući podaci velikim će dijelom potjecati iz industrije, poduzećâ i javnog sektora te će se pohranjivati u raznim sustavima, u prvom redu na računalnim uređajima koji rade na rubu mreže. Zbog toga se otvaraju nove prilike za

[1] Umjetna inteligencija za Europu, COM(2018) 237 final.
[2] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_hr.pdf

Europu, koja ima vodeći položaj u digitaliziranoj industriji i poslovnim aplikacijama, ali relativno slab položaj u sektoru potrošačkih platformi.

Jednostavno rečeno, umjetna inteligencija skup je tehnologija koje se koriste podacima, algoritmima i računalnom snagom. Napredak u računalstvu i sve veća dostupnost podataka stoga su ključni pokretači današnjeg procvata UI-ja. Europa može povezati svoje tehnološke i industrijske prednosti s visokokvalitetnom digitalnom infrastrukturom i regulatornim okvirom koji se temelji na njezinim temeljnim vrijednostima te tako postati **globalni predvodnik u inovacijama u podatkovnom gospodarstvu i njihovim primjenama** kako je utvrđeno u europskoj podatkovnoj strategiji[3]. Na temelju toga može razviti ekosustav za umjetnu inteligenciju koji će koristi od te tehnologije donijeti cijelom europskom društvu i gospodarstvu:

- **građani** će osjetiti napredak u mnogim područjima, među kojima su poboljšana zdravstvena skrb, rjeđi kvarovi kućanskih aparata, sigurniji i čišći prometni sustavi, bolje javne usluge,
- **poslovanje** će napredovati jer će se, na primjer, u područjima u kojima je Europa osobito napredna (strojevi, promet, kibersigurnost, poljoprivreda, zeleno i kružno gospodarstvo, zdravstvo i sektori s visokom dodanom vrijednosti kao što su moda i turizam) razviti nova generacija proizvoda i usluga, a
- **usluge od javnog interesa** poboljšat će se, primjerice, zbog nižih troškova pružanja usluga (prijevoz, obrazovanje, energetika i gospodarenje otpadom), veće održivosti proizvoda[4] te alata s pomoću kojih će tijela kaznenog progona jamčiti zaštitu građana[5], uz odgovarajuće zaštitne mjere kako bi se poštovala njihova prava i slobode.

S obzirom na velik utjecaj koji umjetna inteligencija može imati na naše društvo te na potrebu da izgradimo povjerenje u nju, europska se umjetna inteligencija nužno mora temeljiti na našim vrijednostima i temeljnim pravima kao što su ljudsko dostojanstvo i zaštita privatnosti.

Nadalje, učinak UI sustava treba razmatrati ne samo s gledišta pojedinca nego i iz perspektive društva u cjelini. Upotreba UI sustava može imati važnu ulogu u postizanju ciljeva održivog razvoja te u podupiranju demokratskog procesa i socijalnih prava. Zahvaljujući nedavnim prijedlozima u okviru europskog zelenog plana[6] Europa je postala predvodnik u rješavanju problema povezanih s klimom i okolišem. Digitalne tehnologije kao što je UI ključni su čimbenik za postizanje ciljeva zelenog plana. S obzirom na sve veću važnost umjetne inteligencije, utjecaj UI sustavâ na okoliš treba na odgovarajući način uzeti u obzir tijekom cijelog životnog ciklusa i u cijelom lancu opskrbe, npr. u pogledu upotrebe resursa za učenje algoritama i pohranu podataka.

Kako bi se postigla ekonomija razmjera i izbjegla fragmentacija jedinstvenog tržišta, potreban je zajednički europski pristup umjetnoj inteligenciji. Pokretanje nacionalnih inicijativa moglo bi ugroziti pravnu sigurnost, oslabiti povjerenje građana i spriječiti razvoj dinamične europske industrije.

[3] COM(2020) 66 final.

[4] Umjetna inteligencija i digitalizacija općenito ključni su pokretači ambicija europskog zelenog plana. Međutim, procjenjuje se da je sektor IKT-a danas odgovoran za više od 2 % svih globalnih emisija. U europskoj digitalnoj strategiji, koja je priložena ovoj Bijeloj knjizi, predlažu se mjere zelene transformacije u digitalnom sektoru.

[5] Alati koji se temelje na umjetnoj inteligenciji mogu pridonijeti boljoj zaštiti građana EU-a od kriminala i terorističkih djela. Takvi bi alati, primjerice, mogli pomoći u prepoznavanju terorističke propagande na internetu, otkrivati sumnjive transakcije pri prodaji opasnih proizvoda, identificirati opasne skrivene predmete ili nezakonite tvari ili proizvode te pomagati građanima u hitnim situacijama, a interventnim službama pri lociranju unesrećenikâ.

[6] COM(2019) 640 final.

U ovoj Bijeloj knjizi predstavljene su političke opcije za stvaranje uvjeta za pouzdan i siguran razvoj umjetne inteligencije u Europi, uz potpuno poštovanje vrijednosti i prava građana EU-a. U nastavku su navedeni glavni sastavni dijelovi ove Bijele knjige.

- Politički okvir kojim se utvrđuju mjere za usklađivanje rada na europskoj, nacionalnoj i regionalnoj razini. Cilj je da se tim okvirom, u partnerskom odnosu privatnog i javnog sektora, mobiliziraju sredstva za uspostavu **„ekosustava izvrsnosti”** uzduž cijelog vrijednosnog lanca, počevši od istraživanja i inovacija, te stvore primjereni poticaji koji će ubrzati uvođenje rješenja koja se temelje na UI-ju, među ostalim u malim i srednjim poduzećima (MSP).
- Glavni elementi budućeg regulatornog okvira za umjetnu inteligenciju u Europi, s pomoću kojeg će se uspostaviti jedinstveni **„ekosustav povjerenja”**. Da bi se to postiglo, okvirom se mora osigurati poštovanje pravila EU-a, uključujući pravila o zaštiti temeljnih prava i prava potrošača, osobito za visokorizične UI sustave kojima se upravlja u EU-u[7]. Uspostava ekosustava povjerenja sama je po sebi cilj politike. Građanima bi on trebao uliti pouzdanje za upotrebu UI rješenja, a poduzećima i javnim organizacijama pružiti pravnu sigurnost pri uvođenju inovacija s pomoću UI-ja. Komisija snažno podupire antropocentrični pristup koji se temelji na Komunikaciji o izgradnji povjerenja u antropocentričnu umjetnu inteligenciju[8] te će u obzir uzeti i primjedbe koje je u fazi pripreme etičkih smjernica iznijela stručna skupina na visokoj razini za umjetnu inteligenciju.

Cilj je europske strategije za podatke, koja je priložena ovoj Bijeloj knjizi, omogućiti Europi da postane najprivlačnije, najsigurnije i najdinamičnije gospodarstvo vođeno podacima na svijetu – da iskoristi potencijal podataka kako bi donosila bolje odluke i poboljšala živote svih svojih građana. U strategiji se iznosi niz mjera politike potrebnih za postizanje tog cilja, uključujući mobilizaciju privatnih i javnih ulaganja. Naposljetku, u izvješću Komisije priloženom ovoj Bijeloj knjizi analizira se utjecaj umjetne inteligencije, interneta stvari i drugih digitalnih tehnologija na zakonodavstvo o sigurnosti i odgovornosti.

2. ISKORIŠTAVANJE PREDNOSTI NA INDUSTRIJSKIM I PROFESIONALNIM TRŽIŠTIMA

Europa je u dobrom položaju da iskoristi potencijal UI-ja, ne samo kao korisnik već i kao tvorac i proizvođač te tehnologije. Ima izvrsne istraživačke centre i inovativna perspektivna poduzeća te vodeći položaj u svijetu u području robotike i u konkurentnim proizvodnim i uslužnim sektorima, koji obuhvaćaju sve od automobilske industrije do zdravstva, energetike, financijskih usluga i poljoprivrede. Izgradila je snažnu računalnu infrastrukturu (npr. računala visokih performansi) koja je ključna za funkcioniranje UI-ja. Europa raspolaže velikom količinom javnih i industrijskih podataka, čiji potencijal zasad nije dovoljno iskorišten. Na cijeni su i njezine prednosti u proizvodnji sigurnih i zaštićenih digitalnih sustava s niskom potrošnjom energije, koji su ključni za daljnji razvoj UI-ja.

Iskoriste li se kapaciteti EU-a za ulaganje u tehnologije i infrastrukture sljedeće generacije te u digitalne kompetencije kao što je podatkovna pismenost, povećat će se tehnološka suverenost Europe u ključnim razvojnim tehnologijama i infrastrukturama za podatkovno gospodarstvo. Te bi infrastrukture trebale podupirati stvaranje europskih podatkovnih repozitorija koji omogućuju razvoj pouzdane umjetne inteligencije, primjerice one koja se temelji na europskim vrijednostima i pravilima.

[7] Iako će možda biti potrebno uvesti dodatne mjere za sprečavanje i suzbijanje zlouporabe UI-ja u kriminalne svrhe, to nije obuhvaćeno ovom Bijelom knjigom.
[8] COM(2019) 168.

Europa bi svoje prednosti trebala iskoristiti za jačanje položaja u ekosustavima i uzduž vrijednosnog lanca, od određenih sektora proizvodnje hardvera, preko softvera pa sve do usluga. To se u određenoj mjeri već i događa. Europa proizvodi više od četvrtine svih robota za industrijske i profesionalne usluge (npr. za preciznu poljoprivredu, sigurnost, zdravstvo, logistiku) i ima važnu ulogu u razvoju i primjeni softverskih aplikacija za poduzeća i organizacije (aplikacije za poslovanje među poduzećima kao što je softver za upravljanje resursima poduzeća, programi za dizajn i projektiranje) te aplikacija za potporu e-upravi i „inteligentnom poduzetništvu".

Europa predvodi primjenu UI-ja u proizvodnji. Više od polovine najvećih proizvođača u proizvodnim procesima primjenjuje barem jedno UI rješenje[9].

Jedan od razloga za snažan položaj Europe u području istraživanja jest program financiranja EU-a, koji se pokazao ključnim za udruživanje djelovanja, izbjegavanje dupliciranja te poticanje javnih i privatnih ulaganja u državama članicama. U protekle tri godine financiranje EU-a za istraživanje i inovacije u području umjetne inteligencije poraslo je na 1,5 milijardi EUR, što je povećanje od 70 % u odnosu na prethodno razdoblje.

Međutim, ulaganja u istraživanje i inovacije u Europi i dalje su neznatna u usporedbi s javnim i privatnim ulaganjima u drugim dijelovima svijeta. U Europi je 2016. u UI uloženo oko 3,2 milijarde EUR, dok su ulaganja u Sjevernoj Americi iznosila 12,1 milijardu EUR, a u Aziji 6,5 milijardi EUR.[10] Europa mora odgovoriti znatnim povećanjem svojih ulaganja. Koordinirani plan o umjetnoj inteligenciji[11] izrađen zajedno s državama članicama pokazao se kao dobro polazište za jačanje suradnje u području umjetne inteligencije u Europi te za stvaranje sinergija kako bi se maksimalno povećala ulaganja u vrijednosni lanac UI-ja.

3. ISKORIŠTAVANJE BUDUĆIH PRILIKA: NOVI VAL PODATAKA

Iako je Europa trenutačno u slabijem položaju u području potrošačkih aplikacija i internetskih platformi, zbog čega je manje konkurentna kad je riječ o pristupu podacima, događaju se veliki pomaci u vrijednosti i ponovnoj upotrebi podataka među sektorima. Količina podataka koji se proizvode u svijetu brzo raste te se očekuje da će se od 2018. do 2025. povećati sa 33 zetabajta na 175 zetabajtova.[12] Svaki novi val podataka prilika je za Europu da se pozicionira u gospodarstvu vođenom podacima i postane svjetski predvodnik u tom području. Nadalje, način na koji se podaci pohranjuju i obrađuju u sljedećih će se pet godina promijeniti iz temelja. Danas se 80 % obrade i analize podataka u oblaku odvija u podatkovnim centrima i centraliziranoj računalnoj infrastrukturi, a 20 % u pametnim povezanim proizvodima, kao što su automobili, kućanski aparati ili roboti za proizvodnju, te u računalnoj infrastrukturi u blizini korisnika („računalstvo na rubu mreže"). Smatra se da će se do 2025. ti odnosi znatno promijeniti.[13]

Europa je globalni predvodnik u sektoru elektronike s niskom potrošnjom energije, koji je važan za sljedeću generaciju specijaliziranih procesora za UI. Na tom tržištu trenutačno dominiraju sudionici izvan EU-a. To bi se moglo promijeniti zahvaljujući inicijativama kao što je Inicijativa za europski procesor, koja je usmjerena na razvoj računalnih sustava s niskom potrošnjom energije za računalstvo na rubu mreže i računalstvo visokih performansi sljedeće generacije, te radu Zajedničkog poduzeća za

[9] Slijede Japan (30 %) i SAD (28 %). Izvor: CapGemini (2019.).
[10] 10 imperatives for Europe in the age of AI and automation (Deset imperativa za Europu u doba umjetne inteligencije i automatizacije), McKinsey, 2017.
[11] COM(2018) 795.
[12] IDC (2019.).
[13] Gartner (2017.).

ključnu digitalnu tehnologiju, koji bi trebao početi 2021. Europa je na čelu i u području neuromorfnih rješenja[14], koja su idealna za automatizaciju industrijskih procesa (industrija 4.0) i načina prijevoza. Ona mogu poboljšati energetsku učinkovitost za nekoliko redova veličine.

Nedavna postignuća u području kvantnog računalstva dovest će do eksponencijalnog povećanja kapaciteta obrade[15]. Europa može zauzeti vodeći položaj u tom sektoru zahvaljujući svojim akademskim prednostima u kvantnom računalstvu te snažnom položaju europskih proizvođača kvantnih simulatora i programskih okruženja za kvantno računalstvo. Europske inicijative čiji je cilj povećati dostupnost infrastrukture za kvantna testiranja i eksperimente pomoći će u primjeni tih novih kvantnih rješenja u nizu industrijskih i akademskih sektora.

Europa će istodobno i dalje predvoditi napredak u razvoju algoritamskih temelja umjetne inteligencije, oslanjajući se na vlastitu znanstvenu izvrsnost. Potrebno je povezati discipline koje danas rade odvojeno, kao što su strojno i duboko učenje (za koje su karakteristične ograničena mogućnost tumačenja i potreba za velikom količinom podataka za učenje modela i učenje iz korelacija) te simbolički pristupi (u kojima se pravila određuju ljudskom intervencijom). Primjena simboličnog zaključivanja u dubokim neuralnim mrežama mogla bi nam pomoći da lakše objasnimo ishode umjetne inteligencije.

4. EKOSUSTAV IZVRSNOSTI

Kako bi se uspostavio ekosustav izvrsnosti koji može poduprijeti razvoj i uvođenje umjetne inteligencije u gospodarstvu i javnoj upravi EU-a, potrebno je intenzivnije raditi na više razina.

A. SURADNJA S DRŽAVAMA ČLANICAMA

U okviru provedbe strategije za umjetnu inteligenciju donesene u travnju 2018.[16] Komisija je u prosincu 2018. predstavila koordinirani plan za poticanje razvoja i upotrebe umjetne inteligencije u Europi[17] izrađen u suradnji s državama članicama.

U tom je planu predloženo približno 70 zajedničkih mjera za bližu i učinkovitiju suradnju između država članica i Komisije u ključnim područjima kao što su istraživanje, ulaganja, prihvaćenost na tržištu, vještine i talenti, podaci i međunarodna suradnja. Predviđeno je da će se plan provoditi do 2027., uz redovito praćenje i preispitivanje.

Cilj je maksimalno povećati učinak ulaganja u istraživanje, inovacije i uvođenje, ocijeniti nacionalne strategije za UI te nadograditi i proširiti koordinirani plan o umjetnoj inteligenciji s državama članicama.

- *Prva mjera: Komisija će, uzimajući u obzir rezultate javnog savjetovanja o Bijeloj knjizi, državama članicama predložiti da se do kraja 2020. donese revizija koordiniranog plana.*

Financiranjem umjetne inteligencije na razini EU-a trebalo bi privući i objediniti ulaganja u područjima u kojima potrebne mjere nadilaze mogućnosti pojedinih država članica. Cilj je tijekom idućeg desetljeća privući ulaganja u umjetnu inteligenciju u EU-u u ukupnom iznosu većem od 20 milijardi EUR[18] godišnje. Kako bi potaknuo privatna i javna ulaganja, EU će na raspolaganje staviti

[14] Neuromorfno rješenje je svaki vrlo veliki sustav integriranih krugova koji oponaša neurobiološke strukture živčanog sustava.
[15] Kvantna računala moći će u manje od jedne sekunde obrađivati mnogo veće skupove podataka od današnjih najbržih računala, što će omogućiti razvoj novih primjena UI-ja u raznim sektorima.
[16] Umjetna inteligencija za Europu, COM(2018) 237.
[17] Koordinirani plan o umjetnoj inteligenciji, COM(2018) 795.
[18] COM(2018) 237.

sredstva iz programa Digitalna Europa i Obzora Europa te, za potrebe manje razvijenih regija i ruralnih područja, iz europskih strukturnih i investicijskih fondova.

U koordiniranom bi se planu mogla razmotriti i dobrobit društva i okoliša kao ključno načelo za umjetnu inteligenciju. UI sustavi imaju potencijala pridonijeti rješavanju gorućih problema, uključujući klimatske promjene i uništavanje okoliša. Ujedno je važno da se ta rješenja provode na ekološki prihvatljiv način. UI rješenja mogu i trebala bi sama kritički preispitivati upotrebu resursa i potrošnju energije te naučiti donositi odluke koje su pozitivne za okoliš. Komisija će zajedno s državama članicama razmotriti mogućnosti za poticanje i promicanje UI rješenja koja to čine.

B. USMJERAVANJE RADA ISTRAŽIVAČKE I INOVACIJSKE ZAJEDNICE

Europa si ne može priuštiti da centri kompetentnosti i dalje budu rascjepkani kao danas, a da pritom ni jedan od njih ne doseže razinu potrebnu za natjecanje s vodećim ustanovama na svjetskoj razini. Nužno je stvoriti više sinergija i mreža među raznim europskim istraživačkim centrima za UI te uskladiti njihov rad kako bi se podigla razina izvrsnosti, privukli i zadržali najbolji znanstvenici te razvila najbolja tehnologija. Europi je potreban referentni centar za istraživanje, inovacije i stručnost koji bi koordinirao taj rad, bio svjetsko mjerilo izvrsnosti u području umjetne inteligencije te imao sposobnost da privuče ulaganja i najbolje talente u tom području.

Centri i mreže trebali bi se usredotočiti na sektore u kojima Europa ima potencijal postati svjetski predvodnik, kao što su industrija, zdravstvo, promet, financije, poljoprivredno-prehrambeni vrijednosni lanci, energija/okoliš, šumarstvo, promatranje Zemlje i svemir. U svim tim područjima u tijeku je utrka za globalno vodstvo, a Europa nudi znatan potencijal, znanje i stručnost[19]. Jednako je važno uspostaviti infrastrukturu za testiranje i eksperimente koja bi bila potpora razvoju i uvođenju novih primjena UI-ja.

- *Druga mjera: Komisija će olakšati uspostavu centara za izvrsnost i testiranje u kojima se mogu kombinirati europska, nacionalna i privatna ulaganja, po mogućnosti uz primjenu novog pravnog instrumenta. Komisija je predložila da se za potporu svjetski priznatim referentnim centrima za testiranje u Europi izdvoji ambiciozan namjenski iznos u okviru programa Digitalna Europa koji se, prema potrebi, može dopuniti sredstvima za istraživačke i inovacijske aktivnosti iz programa Obzor Europa u okviru višegodišnjeg financijskog okvira za razdoblje 2021.–2027.*

C. VJEŠTINE

Europski pristup umjetnoj inteligenciji morat će se snažno usredotočiti na vještine kako bi se uklonio nedostatak kompetencija.[20] Komisija će uskoro predstaviti poboljšani Program vještina, kojim želi osigurati da svi u Europi mogu imati koristi od zelene i digitalne transformacije gospodarstva EU-a. Među inicijativama mogla bi biti i potpora sektorskim regulatornim tijelima u unapređenju vlastitih vještina u području umjetne inteligencije kako bi mogla djelotvorno i učinkovito provoditi relevantna pravila. Ažurirani Akcijski plan za digitalno obrazovanje pomoći će da se podaci i tehnologije koje se temelje na UI-ju, kao što su učenje i prediktivna analitika, bolje iskoriste za poboljšanje sustava obrazovanja i osposobljavanja i njihovu prilagodbu digitalnom dobu. Planom će se usto pružiti bolji

[19] Mogućnosti za istraživanje i razvoj u području UI-ja pružat će se i u okviru budućeg Europskog fonda za obranu i stalne strukturirane suradnje. Ti bi projekti trebali biti usklađeni sa širim civilnim programima EU-a posvećenima umjetnoj inteligenciji.

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

uvid u umjetnu inteligenciju na svim razinama obrazovanja kako bi se građane pripremilo za donošenje utemeljenih odluka na koje će UI sve više utjecati.

Razvoj vještina potrebnih za rad u području UI-ja i usavršavanje radne snage kako bi bila spremna za transformaciju na valu umjetne inteligencije bit će prioritet revidiranog koordiniranog plana o umjetnoj inteligenciji koji će se izraditi u suradnji s državama članicama. U okviru tog bi se plana popis za ocjenjivanje etičkih smjernica mogao pretvoriti u okvirni nastavni program za razvojne programere umjetne inteligencije, koji će biti dostupan ustanovama za osposobljavanje kao resurs. Osobito bi trebalo nastojati povećati broj žena osposobljenih za rad i zaposlenih u tom području.

Usto, referentni centar za istraživanje i inovacije u području UI-ja u Europi nudio bi prilike kojima bi privlačio talente iz cijelog svijeta. Ujedno bi razvijao i širo izvrsnost u vještinama koje bi se potom uvriježile i njegovale u cijeloj Europi.

- *Treća mjera: Uspostava mreža vodećih sveučilišta i ustanova visokog obrazovanja, uz potporu iz stupa naprednih vještina u okviru programa Digitalna Europa, kako bi se privukli najbolji profesori i znanstvenici i ponudili svjetski priznati diplomski studiji u području umjetne inteligencije.*

Izvedba i upotreba UI sustava na radnome mjestu ne utječu, međutim, samo na usavršavanje već imaju izravne posljedice na radnike i poslodavce. Uključivanje socijalnih partnera bit će ključan čimbenik u primjeni antropocentričnog pristupa umjetnoj inteligenciji na radnome mjestu.

D. USMJERENOST NA MALA I SREDNJA PODUZEĆA

Jednako je važno da MSP-ovi imaju pristup umjetnoj inteligenciji i mogu je upotrebljavati. U tu bi svrhu trebalo dodatno razviti digitalnoinovacijske centre[21] i platformu za umjetnu inteligenciju na zahtjev[22] te poticati suradnju među MSP-ovima. Program Digitalna Europa bit će ključan za postizanje tog cilja. Iako bi svi digitalnoinovacijski centri trebali pružati potporu MSP-ovima u razumijevanju i uvođenju umjetne inteligencije, barem jedan inovacijski centar po državi članici morat će biti visoko specijaliziran za UI.

MSP-ovi i perspektivna nova poduzeća trebat će pristup financiranju kako bi prilagodili procese ili uvodili inovacije s pomoću UI-ja. Osim što će se najavljenim investicijskim pilot-fondom osigurati iznos od 100 milijuna EUR za umjetnu inteligenciju i lance blokova, Komisija planira dodatno povećati pristup financiranju putem fonda InvestEU[23]. Umjetna inteligencija izričito je navedena kao područje koje ispunjava uvjete za primjenu jamstva InvestEU.

- *Četvrta mjera: Komisija će surađivati s državama članicama kako bi barem jedan digitalnoinovacijski centar po državi članici bio visoko specijaliziran za umjetnu inteligenciju. Digitalnoinovacijski centri mogu dobiti potporu u okviru programa Digitalna Europa.*
- *Komisija i Europski investicijski fond u prvom će tromjesečju 2020. pokrenuti pilot-projekt u iznosu od 100 milijuna EUR kako bi se osiguralo financiranje vlasničkim kapitalom za inovativni razvoj umjetne inteligencije. Ovisno o konačnom dogovoru o VFO-u, Komisija namjerava znatno povećati ta sredstva putem fonda InvestEU nakon 2021.*

[21] ec.europe.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities
[22] www.ai4eu.eu
[23] europe.eu/investeu

E. PARTNERSTVO S PRIVATNIM SEKTOROM

Bitno je također da privatni sektor bude u potpunosti uključen u izradu istraživačko-inovacijskih programa te da sudjeluje u potrebnom sufinanciranju. Za to je potrebno uspostaviti sveobuhvatno javno-privatno partnerstvo i zadobiti potporu višeg rukovodstva poduzećâ.

- *Peta mjera: U kontekstu programa Obzor Europa Komisija će uspostaviti novo javno-privatno partnerstvo u području umjetne inteligencije, podataka i robotike radi udruživanja rada, koordinacije istraživanja i inovacija, suradnje s drugim javno-privatnim partnerstvima u programu Obzor Europa i suradnje s prethodno navedenim infrastrukturama za testiranje te digitalnoinovacijskim centrima.*

F. POTICANJE PRIHVAĆANJA UMJETNE INTELIGENCIJE U JAVNOM SEKTORU

Izuzetno je važno da se u javnim upravama, bolnicama, komunalnim i prijevoznim službama, financijskim nadzornim tijelima i drugim područjima od javnog interesa brzo počnu uvoditi proizvodi i usluge koji se oslanjaju na UI. Posebna će se pozornost posvetiti područjima zdravstvene skrbi i prometa u kojima je tehnologija dovoljno razvijena za opsežnu primjenu.

- *Šesta mjera: Komisija će pokrenuti otvorene i transparentne sektorske dijaloge, pri čemu će dati prednost zdravstvenim ustanovama, ruralnim upravama i operaterima javnih usluga, kako bi predstavila akcijski plan za olakšavanje razvoja, eksperimentiranja i uvođenja. Na temelju sektorskih dijaloga pripremit će se posebni program „Uvođenje umjetne inteligencije", kojim će se podupirati javna nabava UI sustava i doprinijeti preobrazbi postupaka javne nabave.*

G. OSIGURAVANJE PRISTUPA PODACIMA I RAČUNALNOJ INFRASTRUKTURI

Područja djelovanja navedena u ovoj Bijeloj knjizi tvore cjelinu s planom koji je iznesen usporedno u okviru europske podatkovne strategije. Izuzetno je važno poboljšati pristup podacima i upravljanje njima. Razvoj UI-ja i drugih digitalnih aplikacija nije moguć bez podataka. Golema količina novih podataka koji će se tek generirati Europi pruža priliku da postane predvodnik u transformaciji na valu podataka i umjetne inteligencije. Promicanjem praksi odgovornog upravljanja podacima i usklađenosti podataka s načelima FAIR pridonijet će se izgradnji povjerenja i osigurati ponovna upotrebljivost podataka[24]. Jednako je važno ulaganje u ključne računalne tehnologije i infrastrukturu.

Komisija je predložila da se u okviru programa Digitalna Europa izdvoji više od 4 milijarde EUR za potporu visokokvalitetnom računalstvu visokih performansi, uključujući računalstvo na rubu mreže i umjetnu inteligenciju, podatkovnu infrastrukturu i infrastrukturu u oblaku. Ti su prioriteti dodatno razrađeni u europskoj podatkovnoj strategiji.

H. MEĐUNARODNI ASPEKTI

Europa je u dobrom položaju da postane svjetski predvodnik u izgradnji saveza na temelju zajedničkih vrijednosti i promicanju etične upotrebe umjetne inteligencije. Rad EU-a na umjetnoj inteligenciji već je utjecao na međunarodne rasprave. Stručna skupina na visokoj razini je u izradu etičkih smjernica uključila niz organizacija izvan EU-a i nekoliko vladinih promatrača. EU je istovremeno intenzivno

[24] Pretraživost, dostupnost, interoperabilnost i ponovna uporaba, kako je navedeno u završnom izvješću i akcijskom planu stručne skupine Komisije za podatke FAIR, 2018., https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf

sudjelovao u izradi etičkih načela OECD-a za umjetnu inteligenciju[25]. Ta je načela naknadno potvrdila skupina G20 u svojoj Ministarskoj izjavi o trgovini i digitalnom gospodarstvu iz lipnja 2019.

EU istodobno prepoznaje važan rad na umjetnoj inteligenciji koji obavljaju drugi multilateralni forumi, uključujući Vijeće Europe, Organizaciju Ujedinjenih naroda za obrazovanje, znanost i kulturu (UNESCO), Organizaciju za gospodarsku suradnju i razvoj (OECD), Svjetsku trgovinsku organizaciju i Međunarodnu telekomunikacijsku uniju (ITU). U Ujedinjenim narodima EU sudjeluje u daljnjem radu na temelju izvješća Skupine na visokoj razini o digitalnoj suradnji, uključujući njezinu preporuku o umjetnoj inteligenciji.

EU će u području umjetne inteligencije nastaviti surađivati sa zemljama sličnih stajališta, ali i s globalnim akterima, uz primjenu pristupa koji se temelji na pravilima i vrijednostima EU-a (npr. podupiranje uzlazne regulatorne konvergencije, pristup ključnim resursima, uključujući podatke, stvaranje ravnopravnih uvjeta). Komisija će pomno pratiti politike trećih zemalja koje ograničavaju protok podataka i nastojat će ukloniti nepotrebna ograničenja u bilateralnim trgovinskim pregovorima te mjerama u kontekstu Svjetske trgovinske organizacije. Komisija je uvjerena da se međunarodna suradnja u području UI-ja mora temeljiti na pristupu kojim se promiče poštovanje temeljnih prava, uključujući ljudsko dostojanstvo, pluralizam, uključenost, nediskriminaciju i zaštitu privatnosti i osobnih podataka[26] te će nastojati promicati svoje vrijednosti u svijetu[27]. Nesumnjivo je i da odgovorni razvoj i upotreba umjetne inteligencije mogu biti pokretačka snaga za postizanje ciljeva održivog razvoja i promicanje Programa održivog razvoja do 2030.

5. EKOSUSTAV POVJERENJA: REGULATORNI OKVIR ZA UMJETNU INTELIGENCIJU

Kao što je to slučaj sa svakom novom tehnologijom, upotreba UI-ja sa sobom donosi i prilike i rizike. Građani se boje da neće moći obraniti svoja prava i sigurnost zbog asimetrije informacija u algoritamskom donošenju odluka, a poduzeća su zabrinuta zbog pravne nesigurnosti. Iako umjetna inteligencija može doprinijeti sigurnosti građana i omogućiti im da ostvaruju temeljna prava, građani se boje da bi mogla imati neželjene učinke ili se čak upotrebljavati u zlonamjerne svrhe. Tu zabrinutost treba ukloniti. Nadalje, uz nedostatna ulaganja i vještine, nedostatak povjerenja glavni je čimbenik koji koči širu primjenu UI-ja.

Zbog toga je Komisija 25. travnja 2018. donijela strategiju za umjetnu inteligenciju[28], u kojoj se usporedno s povećanjem ulaganja u istraživanje, inovacije i kapacitete umjetne inteligencije diljem EU-a razmatraju i njezini socioekonomski aspekti. S državama članicama izradila je koordinirani plan[29] radi usklađivanja strategija. Komisija je usto osnovala stručnu skupinu na visokoj razini koja je u travnju 2019. objavila Smjernice o pouzdanoj umjetnoj inteligenciji[30].

Komisija je objavila Komunikaciju[31] u kojoj je pozdravila sedam ključnih zahtjeva utvrđenih u Smjernicama stručne skupine na visokoj razini, a to su:

- ljudsko djelovanje i nadzor,

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

[26] U okviru Instrumenta za partnerstvo Komisija će financirati projekt vrijedan 2,5 milijuna EUR kojim će se olakšati suradnja s partnerima istomišljenicima u cilju promicanja etičkih smjernica EU-a u području umjetne inteligencije te donošenja zajedničkih načela i operativnih zaključaka.

[27] Predsjednica Von der Leyen, Ambicioznija Unija – Moj plan za Europu, str. 18.

[28] COM(2018) 237.

[29] COM(2018) 795.

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

[31] COM(2019) 168.

- tehnička stabilnost i sigurnost,
- privatnost i upravljanje podacima,
- transparentnost,
- raznolikost, nediskriminacija i pravednost,
- dobrobit društva i okoliša te
- odgovornost.

Smjernice usto sadržavaju popis za procjenu za praktičnu primjenu u poduzećima. U drugoj polovini 2019. taj je popis za procjenu u praksi isprobalo više od 350 organizacija, koje su o tome poslale povratne informacije. Skupina na visokoj razini trenutačno revidira Smjernice imajući u vidu te povratne informacije i taj će rad dovršiti do lipnja 2020. Najvažniji zaključak izveden iz prikupljenih povratnih informacija jest taj da, unatoč tome što su neki zahtjevi već uvršteni u postojeće pravne ili regulatorne sustave, oni koji se odnose na transparentnost, sljedivost i ljudski nadzor nisu posebno obuhvaćeni postojećim zakonodavstvom u mnogim gospodarskim sektorima.

Nadovezujući se na taj skup neobvezujućih smjernica stručne skupine na visokoj razini i u skladu s političkim smjernicama predsjednice, jasan europski regulatorni okvir pridonio bi izgradnji povjerenja potrošača i poduzeća u UI, čime bi se ubrzalo uvođenje tehnologije. Takav regulatorni okvir trebao bi biti usklađen s drugim mjerama za promicanje inovacijskih kapaciteta i konkurentnosti Europe u tom području. Njime se ujedno moraju jamčiti ishodi koji su optimalni za društvo, okoliš i gospodarstvo te usklađenost sa zakonodavstvom, načelima i vrijednostima EU-a. To je posebno važno u područjima u kojima bi prava građana mogla biti najizravnije pogođena, primjerice u slučaju UI rješenja za primjenu u tijelima kaznenog progona i pravosuđu.

Razvojni programeri UI-ja i subjekti koji ga primjenjuju već podliježu europskom zakonodavstvu o temeljnim pravima (npr. zaštita podataka, privatnost, nediskriminacija) i zaštiti potrošača te pravilima o sigurnosti proizvoda i odgovornosti za njih. Potrošači očekuju jednaku razinu sigurnosti i poštovanje prava bez obzira na to oslanja li se proizvod ili sustav na UI ili ne. Međutim, određena obilježja umjetne inteligencije (npr. netransparentnost) mogu otežati primjenu i provedbu tog zakonodavstva. Zbog toga je potrebno ispitati je li postojeće zakonodavstvo u stanju otkloniti rizike koje donosi UI i može li se ono učinkovito provoditi te je li potrebno prilagoditi postojeće ili donijeti novo zakonodavstvo.

S obzirom na brz razvoj umjetne inteligencije, u regulatornom se okviru mora ostaviti prostora za buduće promjene. Eventualne izmjene trebalo bi ograničiti na jasno definirane probleme za koje postoje izvediva rješenja.

Države članice ukazuju na to da trenutačno ne postoji zajednički europski okvir. Njemačka komisija za etiku podataka pozvala je na uspostavu sustava reguliranja utemeljenog na riziku s pet razina koje bi sezale od nepostojanja regulacije za najneškodljivije UI sustave do potpune zabrane za one najopasnije. Danska je upravo predstavila prototip certifikata za etiku podataka. Malta je uvela dobrovoljni sustav certificiranja za umjetnu inteligenciju. Ako EU ne uspije osigurati pristup na razini EU-a, postoji stvaran rizik od rascjepkanosti unutarnjeg tržišta, što bi ugrozilo ciljeve povjerenja, pravne sigurnosti i prihvaćenosti na tržištu.

Solidan europski regulatorni okvir za pouzdanu umjetnu inteligenciju zaštitit će sve europske građane i pomoći u stvaranju neometanog unutarnjeg tržišta u cilju daljnjeg razvoja i uvođenja UI-ja te jačanja europske industrijske osnove u području umjetne inteligencije.

A. *DEFINICIJA PROBLEMA*

Iako umjetna inteligencija može biti od velike koristi, među ostalim i zato što proizvode i procese čini sigurnijima, isto tako može nanijeti štetu. Ta šteta može biti materijalna (sigurnost i zdravlje pojedinaca, uključujući gubitak života, oštećenje imovine) i nematerijalna (gubitak privatnosti, ograničavanje prava na slobodu izražavanja, povreda ljudskog dostojanstva, diskriminacija, primjerice pri zapošljavanju) te može biti povezana s brojnim rizicima. Regulatorni okvir trebao bi se usredotočiti na smanjenje različitih rizika od moguće štete, osobito onih najozbiljnijih.

Glavni rizici povezani s upotrebom UI-ja odnose se na primjenu pravila za zaštitu temeljnih prava (uključujući zaštitu osobnih podataka i privatnosti te nediskriminaciju) te na pitanja povezana sa sigurnošću[32] i odgovornošću.

Rizici za temeljna prava, uključujući zaštitu osobnih podataka i privatnosti te nediskriminaciju

Upotreba umjetne inteligencije može utjecati na vrijednosti na kojima je EU utemeljen i dovesti do kršenja temeljnih prava[33], uključujući pravo na slobodu izražavanja, slobodu okupljanja, ljudsko dostojanstvo, nediskriminaciju na temelju spola, rasnog ili etničkog podrijetla, vjere ili uvjerenja, invaliditeta, dobi ili spolne orijentacije, kako je primjenjivo u određenim područjima, zaštitu osobnih podataka i privatnog života[34] ili pravo na djelotvoran pravni lijek i pošteno suđenje te zaštitu potrošača. Ti rizici mogu proizaći iz nedostataka u projektiranju UI sustavâ (uključujući nedostatke u pogledu ljudskog nadzora) ili zbog upotrebe podataka bez ispravljanja moguće pristranosti (npr. sustav je učio samo ili uglavnom iz podataka o muškarcima, pa za žene ne daje optimalne rezultate).

Umjetna inteligencija može obavljati mnoge funkcije koje su prije mogli obavljati samo ljudi. Na građane i pravne subjekte zbog toga će se sve više primjenjivati mjere i odluke koje donose UI sustavi ili se donose uz njihovu pomoć, a koje ponekad može biti teško razumjeti i osporavati ako je potrebno. Nadalje, zahvaljujući UI-ju moguće je podrobnije pratiti i analizirati svakodnevne navike ljudi. Primjerice, postoji potencijalni rizik da bi državna tijela ili drugi subjekti mogli upotrebljavati UI za masovni nadzor, a poslodavci za praćenje ponašanja zaposlenika, što bi bilo kršenje pravila EU-a o zaštiti podataka. Zbog sposobnosti analiziranja velikih količina podataka i utvrđivanja poveznica među njima UI se usto može upotrebljavati za praćenje i deanonimizaciju podataka o osobama, pa su mogući novi rizici za zaštitu osobnih podataka čak i kad je riječ o skupovima podataka koji sami po sebi ne sadržavaju osobne podatke. Umjetnu inteligenciju upotrebljavaju i internetski posrednici kako bi svojim korisnicima dali probrane informacije i moderirali sadržaj. Obrađeni podaci, izvedba aplikacija i opseg u kojem je moguća ljudska intervencija mogu utjecati na pravo na slobodu izražavanja, zaštitu osobnih podataka, privatnost i političke slobode.

[32] To uključuje pitanja kibersigurnosti, pitanja povezana s primjenom UI-ja u kritičnoj infrastrukturi ili zlonamjernu upotrebu UI-ja.

[33] Istraživanje Vijeća Europe pokazuje da bi upotreba umjetne inteligencije mogla utjecati na velik broj temeljnih prava, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

[34] Ti su rizici obuhvaćeni Općom uredbom o zaštiti podataka i Direktivom o e-privatnosti (novom uredbom o e-privatnosti o kojoj se pregovara), ali možda će biti potrebno ispitati donose li UI sustavi dodatne rizike. Komisija će kontinuirano pratiti i procjenjivati primjenu Opće uredbe o zaštiti podataka.

Pri predviđanju ponavljanja kaznenih djela određeni algoritmi umjetne inteligencije mogu biti pristrani s obzirom na spol i rasu, što je vidljivo iz različitih vjerojatnosti ponavljanja kaznenih djela koje su prognozirane za žene i muškarce ili za državljane i strance. *Izvor: Tolan S., Miron M., Gomez E. i Castillo C., „Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia" („Zašto strojno učenje može uzrokovati nepravdu: dokazi na temelju procjene rizika u maloljetničkom pravosuđu u Kataloniji"), nagrada za najbolji rad, Međunarodna konferencija o umjetnoj inteligenciji i pravu, 2019.*

Određeni programi umjetne inteligencije za analizu lica pokazuju pristranost s obzirom na spol i rasu jer gotovo ne griješe pri određivanju spola muškaraca svijetle puti, ali uvelike griješe pri određivanju spola tamnoputih žena. Izvor: *Joy Buolamwini, Timnit Gebru, Proceedings of the 1st Conference on Fairness, Accountability and Transparency (Zbornik radova Prve konferencije o pravednosti, odgovornosti i transparentnosti), PMLR 81:77-91, 2018.*

Pristranost i diskriminacija inherentni su rizici svake društvene ili gospodarske aktivnosti. Odluke koje donose ljudi nisu imune na pogreške i pristranost. Međutim, ista takva pristranost u sustavu UI-ja mogla bi imati mnogo šire posljedice te utjecati na mnoge ljude i diskriminirati ih ako nema mehanizama društvene kontrole koji upravljaju ljudskim ponašanjem[35]. To se može dogoditi i ako UI sustav „uči" tijekom rada. U takvim slučajevima, ako ishod nije bilo moguće spriječiti ili predvidjeti tijekom projektiranja, rizici neće proizlaziti iz nedostataka u temeljnom konceptu sustava, nego iz praktičnih učinaka korelacija ili uzoraka koje sustav prepozna u velikom skupu podataka.

Specifičnosti mnogih UI tehnologija, uključujući netransparentnost („učinak crne kutije"), složenost, nepredvidljivost i djelomično autonomno ponašanje, mogu otežati provjeru poštovanja postojećih pravila EU-a namijenjenih zaštiti temeljnih prava i otežati njihovu učinkovitu provedbu. Naime, provedbena tijela i oštećene osobe možda neće imati kako provjeriti na koji je način uz pomoć UI-ja određena odluka donesena niti jesu li pritom poštovana relevantna pravila. Pojedinci i pravni subjekti mogu se suočiti s poteškoćama u učinkovitom pristupu pravosuđu u situacijama u kojima su im takve odluke naštetile.

Rizici za sigurnost i učinkovito funkcioniranje sustava odgovornosti

UI tehnologije mogu predstavljati nove sigurnosne rizike za korisnike kad su ugrađene u proizvode i usluge. Na primjer, zbog nedostataka u tehnologiji prepoznavanja predmeta autonomni automobil može pogrešno identificirati predmet na cesti i prouzročiti nesreću s ozljedama i materijalnom štetom. Kao i kod rizika za temeljna prava, ti rizici mogu biti uzrokovani nedostacima u konceptu UI tehnologije, povezani s nedovoljnom dostupnosti i kvalitetom podataka ili s drugim problemima koji proizlaze iz strojnog učenja. Iako neki od tih rizika nisu ograničeni na proizvode i usluge koji se oslanjaju na UI, primjena umjetne inteligencije rizike može povećati ili pogoršati.

[35] Savjetodavni odbor Komisije za jednake mogućnosti žena i muškaraca trenutačno priprema „Mišljenje o umjetnoj inteligenciji" u kojem se, među ostalim, analiziraju učinci umjetne inteligencije na rodnu ravnopravnost, a očekuje se da će ga Odbor donijeti početkom 2020. Veza umjetne inteligencije i rodne ravnopravnosti spominje se i u Strategiji EU-a za rodnu ravnopravnost za razdoblje 2020. – 2024. Očekuje se da će Europska mreža tijela za ravnopravnost (Equinet) početkom 2020. objaviti izvješće „Reguliranje umjetne inteligencije: nova uloga tijela za ravnopravnost – novi izazovi za jednakost i nediskriminaciju zbog povećane digitalizacije i upotrebe umjetne inteligencije" (autori Robin Allen i Dee Master).

Zbog nepostojanja jasnih sigurnosnih odredbi za suzbijanje tih rizika može nastati pravna nesigurnost ne samo za pojedince već i za poduzeća koja svoje proizvode s UI-jem stavljaju na tržište u EU-u. Tijela za nadzor tržišta i tijela za provedbu mogu se naći u situaciji u kojoj nije jasno mogu li intervenirati jer možda nisu ovlaštena djelovati i/ili nemaju odgovarajuće tehničke sposobnosti za inspekciju sustava[36]. Zbog pravne se nesigurnosti stoga može smanjiti ukupna razina sigurnosti i ugroziti konkurentnost europskih poduzeća.

Ako se sigurnosni rizici ostvare, zbog nepostojanja jasnih zahtjeva i prethodno navedenih karakteristika UI tehnologija bit će teško pratiti potencijalno problematične odluke donesene uz sudjelovanje UI sustavâ. To bi pak osobama koje su pretrpjele štetu moglo otežati dobivanje naknade na temelju postojećeg zakonodavstva EU-a i nacionalnog zakonodavstva o odgovornosti.[37]

U skladu s Direktivom o odgovornosti za proizvode za štetu prouzročenu neispravnim proizvodom odgovoran je proizvođač. Međutim, kad je riječ o sustavu temeljenom na UI-ju, kao što su autonomni automobili, može biti teško dokazati neispravnost proizvoda, nastalu štetu i uzročnu vezu između njih. Usto, nije posve jasno kako se i u kojoj mjeri Direktiva o odgovornosti za proizvode primjenjuje u slučaju određenih vrsta nedostataka, na primjer ako oni proizlaze iz nedostataka u kibersigurnosti proizvoda.

Stoga se, kao i na temeljna prava, i na pitanja povezana sa sigurnošću i odgovornošću primjenjuju poteškoće u utvrđivanju potencijalno problematičnih odluka koje donose UI sustavi. Oštećene osobe, na primjer, možda neće moći pribaviti dokaze potrebne za sudski postupak te će im možda biti dostupne manje učinkovite mogućnosti pravne zaštite u usporedbi sa situacijama u kojima je šteta prouzročena tradicionalnim tehnologijama. Ti će se rizici povećati s raširenijom upotrebom UI-ja.

B. MOGUĆE PRILAGODBE POSTOJEĆEG ZAKONODAVNOG OKVIRA EU-A S OBZIROM NA UMJETNU INTELIGENCIJU

Opsežan skup postojećeg zakonodavstva EU-a, uključujući sektorske propise, o sigurnosti proizvoda i odgovornosti za njih[38], dodatno upotpunjen nacionalnim propisima, relevantan je i potencijalno primjenjiv za niz perspektivnih primjena UI-ja.

Kad je riječ o zaštiti temeljnih i potrošačkih prava, zakonodavni okvir EU-a čine propisi kao što su Direktiva o rasnoj jednakosti[39], Direktiva o jednakom postupanju pri zapošljavanju i obavljanju zanimanja[40], direktive o jednakom postupanju prema muškarcima i ženama u pitanjima zapošljavanja te pristupa robi i uslugama[41], nekoliko propisa o pravima potrošača[42] te propisi o zaštiti osobnih

[36] Kao primjer može se navesti pametni sat za djecu. Taj proizvod možda neće uzrokovati izravnu štetu djetetu koje ga nosi, ali ako nema minimalnu razinu sigurnosti, lako ga se može upotrebljavati kao sredstvo za pristup djetetu. Tijelima za nadzor tržišta može biti teško intervenirati u slučajevima u kojima rizik nije povezan s proizvodom kao takvim.

[37] Posljedice umjetne inteligencije, interneta stvari i drugih digitalnih tehnologija na zakonodavstvo o sigurnosti i odgovornosti analiziraju se u izvješću Komisije priloženom ovoj Bijeloj knjizi.

[38] Pravni okvir EU-a o sigurnosti proizvoda čine Direktiva o općoj sigurnosti proizvoda (Direktiva 2001/95/EZ), kao zaštitni mehanizam, te niz sektorskih propisa za razne kategorije proizvoda, od strojeva, aviona i automobila do igračaka i medicinskih uređaja, kojima se nastoji postići visoka razina sigurnosti i zdravstvene ispravnosti. Propise o odgovornosti za proizvode upotpunjuju različiti sustavi građanskopravne odgovornosti za štetu od proizvoda ili usluga.

[39] Direktiva 2000/43/EZ.

[40] Direktiva 2000/78/EZ.

[41] Direktiva 2004/113/EZ, Direktiva 2006/54/EZ.

podataka i privatnosti, ponajprije Opća uredba o zaštiti podataka i drugi sektorski propisi kao što je Direktiva o zaštiti podataka pri izvršavanju zakonodavstva[43]. Od 2025. primjenjivat će se i odredbe o zahtjevima u pogledu pristupačnosti robe i usluga utvrđene u Europskom aktu o pristupačnosti[44]. Usto, temeljna se prava moraju poštovati i pri primjeni drugog zakonodavstva EU-a, među ostalim u područjima financijskih usluga, migracija ili odgovornosti internetskih posrednika.

Premda se zakonodavstvo EU-a u načelu nastavlja primjenjivati u cijelosti bez obzira na prisutnost umjetne inteligencije, važno je procijeniti može li se njegovom provedbom odgovoriti na rizike koji nastaju primjenom UI sustava ili je pojedine pravne instrumente potrebno prilagoditi.

Primjerice, gospodarski dionici ostaju u potpunosti odgovorni za usklađenost UI-ja s postojećim propisima za zaštitu potrošača; zabranjeno je svako algoritamsko iskorištavanje ponašanja potrošača protivno postojećim propisima i svi će se prekršaji primjereno kazniti.

Komisija smatra da bi se zakonodavni okvir mogao prilagoditi s obzirom na sljedeće rizike i situacije:

- *Djelotvorna primjena i provedba postojećeg zakonodavstva EU-a i nacionalnog zakonodavstva*: glavna obilježja UI-ja dovode u pitanje osiguravanje pravilne primjene i provedbe zakonodavstva EU-a i nacionalnog zakonodavstva. Nedostatak transparentnosti (netransparentnost UI-ja) otežava prepoznavanje i dokazivanje mogućih kršenja propisa, među ostalim i odredbi kojima se štite temeljna prava, pripisivanje odgovornosti i ispunjavanje uvjeta za naknadu štete. Prema tome, za djelotvornu primjenu i provedbu možda će biti potrebno prilagoditi ili razjasniti postojeće propise u određenim područjima, primjerice u području odgovornosti kao što je podrobnije objašnjeno u izvješću priloženom ovoj Bijeloj knjizi.

- *Ograničeno područje primjene postojećeg zakonodavstva EU-a*: zakonodavstvo EU-a o sigurnosti proizvoda usmjereno je ponajprije na stavljanje proizvoda na tržište. Premda u okviru tog zakonodavstva softver koji je dio gotovog proizvoda mora biti u skladu s relevantnim propisima o sigurnosti proizvoda, upitno je odnosi li se ono i na samostalni softver. Iznimka su određeni sektori s izričitim pravilima[45]. Važeći opći propisi EU-a o sigurnosti odnose se na proizvode, a ne na usluge, pa se stoga u načelu ne odnose ni na usluge koje se temelje na UI tehnologiji (npr. zdravstvene usluge, financijske usluge, prometne usluge).

- *Promjenjiva funkcionalnost sustavâ umjetne inteligencije*: integracijom softvera, uključujući UI, u proizvode može se promijeniti funkcioniranje takvih proizvoda i sustava tijekom njihova životnog ciklusa. To osobito vrijedi za sustave kojima je potrebno često ažuriranje softvera ili koji se oslanjaju na strojno učenje. Zbog tih se mogućnosti mogu pojaviti novi rizici, kojih nije bilo kad je sustav stavljen na tržište. U sadašnjim propisima, uglavnom usmjerenima na sigurnosne rizike prisutne u trenutku stavljanja na tržište, ti rizici nisu primjereno regulirani.

---

[42] Primjerice, Direktiva o nepoštenoj poslovnoj praksi (Direktiva 2005/29/EZ) i Direktiva o pravima potrošača (Direktiva 2011/83/EZ).

[43] Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka

[44] Direktiva (EU) 2019/882 o zahtjevima za pristupačnost proizvoda i usluga.

[45] Primjerice, softver koji je proizvođač namijenio za medicinske svrhe smatra se medicinskim proizvodom prema Uredbi o medicinskim proizvodima (Uredba (EU) 2017/745).

- *Nesigurnost u pogledu podjele odgovornosti među različitim gospodarskim subjektima u opskrbnom lancu*: prema zakonodavstvu EU-a o sigurnosti proizvoda odgovornost je općenito na proizvođaču proizvoda stavljenog na tržište, što obuhvaća i sve sastavne dijelove, npr. UI sustave. Pravila, međutim, mogu postati nejasna ako, primjerice, nakon stavljanja proizvoda na tržište UI rješenje u njega doda strana koja nije proizvođač. Usto, propisima EU-a o odgovornosti za proizvode uređuje se odgovornost proizvođača, a reguliranje odgovornosti ostalih sudionika u opskrbnom lancu prepušteno je nacionalnim zakonodavstvima.

- *Promjene u konceptu sigurnosti:* zbog upotrebe UI-ja u proizvodima i uslugama mogu se pojaviti rizici koji u zakonodavstvu EU-a trenutačno nisu izričito uređeni. To mogu biti rizici povezani s kiberprijetnjama, rizici za osobnu sigurnost (zbog npr. novih primjena UI-ja u kućanskim aparatima), rizici zbog gubitka povezivosti itd. Mogu biti prisutni pri stavljanju proizvoda na tržište, ali i nastati zbog ažuriranja softvera ili samostalnog učenja tijekom upotrebe proizvoda. EU bi trebao u potpunosti iskoristiti sve što mu je na raspolaganju da poveća fond podataka o potencijalnim rizicima povezanima s primjenama UI-ja, među ostalim, osloniti se na iskustvo Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA) za procjenu stanja prijetnji u području umjetne inteligencije.

Kako je već spomenuto, nekoliko država članica razmatra mogućnosti da nacionalnim zakonodavstvom uredi pitanja koja donosi UI. Zbog toga postoji rizik od fragmentiranja jedinstvenog tržišta. Neujednačenost nacionalnih pravila može stvoriti prepreke poduzećima koja žele prodavati i primjenjivati UI sustave na jedinstvenom tržištu. Zajednički pristup na razini EU-a europskim bi poduzećima omogućio nesmetan pristup jedinstvenom tržištu i pridonio njihovoj konkurentnosti na svjetskim tržištima.

Izvješće o utjecaju umjetne inteligencije, interneta stvari i robotike na sigurnost i odgovornost

U tom izvješću, priloženom ovoj Bijeloj knjizi, analizira se relevantni pravni okvir. Navode se nesigurnosti u vezi s primjenom tog okvira na specifične rizike primjene UI sustava i drugih digitalnih tehnologija.

Zaključuje se da je sadašnjim zakonodavstvom o sigurnosti proizvoda već podržan prošireni koncept sigurnosti, odnosno zaštita od svih vrsta rizika ovisno o načinu upotrebe određenog proizvoda. Ipak, radi veće pravne sigurnosti mogle bi se unijeti izričite odredbe o novim rizicima koje donose perspektivne digitalne tehnologije.

- Autonomnost određenih UI sustava tijekom njihova životnog ciklusa može uzrokovati važne promjene proizvoda koje utječu na sigurnost i zbog njih može biti potrebna nova procjena rizika. Usto, ljudski bi nadzor mogao biti potreban kao zaštitna mjera tijekom izrade i cijelog životnog ciklusa proizvoda i UI sustava.
- Moglo bi se razmotriti i da se, prema potrebi, uvedu izričite obveze za proizvođače kad je riječ o rizicima za psihičko zdravlje korisnika (npr. zbog interakcije s čovjekolikim robotima).
- U zakonodavstvu EU-a o sigurnosti proizvoda mogli bi se propisati konkretni zahtjevi u pogledu sigurnosnih rizika zbog loših podataka u fazi izrade te mehanizmi kojima bi se osiguralo održavanje kvalitete podataka tijekom upotrebe proizvoda i sustava s umjetnom inteligencijom.
- Netransparentnost sustava na bazi algoritama mogla bi se regulirati zahtjevima u pogledu transparentnosti.
- Postojeća će pravila možda trebati prilagoditi i razjasniti za slučaj samostalnog softvera koji se kao takav stavlja na tržište ili učitava u proizvod nakon njegova stavljanja na tržište, ako to utječe na sigurnost.
- S obzirom na to da su zbog novih tehnologija opskrbni lanci sve složeniji, pravna bi se sigurnost mogla postići odredbama kojima se izričito zahtijeva suradnja između gospodarskih subjekata u opskrbnom lancu i korisnika.

Karakteristike perspektivnih digitalnih tehnologija kao što su UI, internet stvari i robotika mogle bi dovesti u pitanje pravne okvire za odgovornost i smanjiti im djelotvornost. Neke od tih karakteristika mogle bi otežati utvrđivanje krivca za štetu, što je u skladu s većinom nacionalnih pravila nužno za naknadu štete na temelju krivnje. To bi moglo znatno povećati troškove oštećenim osobama i otežati podnošenje ili dokazivanje tužbe za naknadu štete protiv osoba koje nisu proizvođači.

- Osobama koje su pretrpjele štetu nastalu zbog djelovanja UI sustava treba pružiti istu razinu zaštite kao osobama koje su pretrpjele štetu izazvanu drugim tehnologijama, a istodobno bi trebalo omogućiti nastavak razvoja tehnoloških inovacija.
- Sve bi mogućnosti za ostvarenje tog cilja trebalo pomno odvagati, uključujući moguće izmjene Direktive o odgovornosti za proizvode i moguće daljnje ciljano usklađivanje nacionalnih pravila o odgovornosti. Komisija, primjerice, prikuplja stajališta o tome treba li i u kojoj mjeri ublažiti posljedice složenosti prilagodbom tereta dokaza u nacionalnim pravilima o odgovornosti za štetu prouzročenu radom UI rješenja.

Na temelju prethodne rasprave Komisija zaključuje da bi, uz moguće prilagodbe postojećeg zakonodavstva, moglo biti potrebno novo zakonodavstvo o umjetnoj inteligenciji kako bi se pravni okvir EU-a prilagodio aktualnim i očekivanim tehnološkim i trgovinskim promjenama.

C. PODRUČJE PRIMJENE BUDUĆEG REGULATORNOG OKVIRA EU-A

Za budući posebni regulatorni okvir za umjetnu inteligenciju ključno je odrediti područje njegove primjene. Radna je hipoteza da bi se taj okvir primjenjivao na proizvode i usluge što se oslanjaju na UI. Zato bi umjetnu inteligenciju trebalo jasno definirati za potrebe ove Bijele knjige i eventualne buduće inicijative za oblikovanje politike.

Komisija je umjetnu inteligenciju prvi put definirala u Komunikaciji o umjetnoj inteligenciji za Europu[46]. Stručna skupina na visokoj razini tu je definiciju proširila[47].

U bilo kojem novom pravnom instrumentu definicija umjetne inteligencije morat će biti dovoljno prilagodljiva da obuhvati tehnički napredak i pritom dovoljno precizna da pruži potrebnu pravnu sigurnost.

Za potrebe ove Bijele knjige, kao i svih eventualnih budućih rasprava o inicijativama politike, čini se važno objasniti glavne elemente koji čine umjetnu inteligenciju, odnosno „podatke” i „algoritme”. Umjetna inteligencija može biti ugrađena u hardver. U slučaju tehnika strojnog učenja, koje su podskup algoritama UI-ja, algoritme učimo da na temelju određenog skupa podataka donose zaključke o određenim pravilnostima radi određivanja radnji potrebnih za postizanje zadanog cilja. Algoritmi mogu nastaviti učiti dok su u upotrebi. Premda proizvodi koji se temelje na UI-ju mogu djelovati autonomno opažanjem svoje okoline i bez praćenja unaprijed određenog skupa uputa, ponašanje im uglavnom odrede i ograniče proizvođači. Ljudi određuju i programiraju ciljeve prema kojima bi UI sustav trebao optimirati rad.

> Pri autonomnoj vožnji, primjerice, algoritam u stvarnom vremenu koristi podatke iz automobila (brzina, potrošnja goriva, podaci iz amortizera itd.) i iz senzora koji prate cijelu okolinu automobila (cestu, prometne znakove, druga vozila, pješake itd.) kako bi zaključio kuda bi i kojom brzinom automobil trebao ići da bi stigao do odredišta. Na temelju opaženih podataka algoritam se prilagođava stanju na cesti i vanjskim uvjetima, što uključuje ponašanje drugih vozača, kako bi odabrao najugodniju i najsigurniju vožnju.

EU ima strog pravni okvir za, među ostalim, zaštitu potrošača, borbu protiv nepoštenih trgovačkih praksi i zaštitu osobnih podataka i privatnosti. Usto, pravna stečevina sadržava posebna pravila za određene sektore (npr. zdravstvo, promet). Te će se postojeće odredbe prava EU-a nastaviti primjenjivati u vezi s UI-jem, međutim možda će biti potrebna određena ažuriranja tog okvira kako bi se uzela u obzir digitalna transformacija i primjena UI-ja (vidjeti odjeljak B). Zbog toga će aspekti koji

[46] COM(2018) 237 final, str. 1.: „Izrazom umjetna inteligencija (UI) označavaju se sustavi koji pokazuju inteligentno ponašanje tako što analiziraju svoje okruženje i izvode radnje – uz određeni stupanj autonomije – radi postizanja određenih ciljeva.
Sustavi temeljeni na umjetnoj inteligenciji mogu biti samo softverski i djelovati u virtualnom svijetu (npr. glasovni asistent, softver za analizu slike, tražilice, sustavi prepoznavanja glasa i lica) ili UI može biti ugrađen u hardverske uređaje (npr. napredni roboti, autonomni automobili, dronovi ili aplikacije za internet stvari).”

[47] Stručna skupina na visokoj razini, Definicija umjetne inteligencije, str. 8.: „Sustavi umjetne inteligencije (UI) su softverski (te moguće i hardverski) sustavi koje je projektirao čovjek i koji, kad im se zada složeni cilj, djeluju u fizičkoj ili digitalnoj dimenziji opažanjem okoline prikupljanjem podataka, tumačenjem prikupljenih strukturiranih ili nestrukturiranih podataka, zaključivanjem na temelju znanja ili obrade informacija iz tih podataka i odlučivanjem o radnjama koje je najbolje učiniti da se postigne zadani cilj. UI sustavi mogu koristiti simbolička pravila ili naučiti numerički model i mogu prilagođavati ponašanje analizirajući kako su njihove prethodne radnje utjecale na okolinu.”

su već pokriveni postojećim horizontalnim ili sektorskim propisima (npr. o medicinskim uređajima[48], u prometnim sustavima) ostati uređeni tim propisima.

U načelu bi novi regulatorni okvir za UI trebao biti učinkovit tako da se ostvare njegovi ciljevi, ali istodobno ne toliko preskriptivan da stvori neproporcionalno opterećenje, osobito MSP-ovima. Kako bi postigla tu ravnotežu, Komisija smatra da bi se njezin pristup trebao temeljiti na procjeni rizika.

Pristup na temelju rizika važna je pomoć za postizanje proporcionalne regulatorne intervencije. Potrebni su, međutim, jasni kriteriji za razlikovanje različitih primjena UI-ja, osobito kad je riječ o pitanju jesu li „visokorizične"[49]. Određivanje visokorizičnih primjena trebalo bi biti jasno, lako razumljivo i primjenjivo za sve uključene strane. No čak i ako neka primjena UI-ja nije svrstana među visokorizične, za nju u cijelosti i dalje vrijede postojeća pravila EU-a

Komisija smatra da bi visokorizičnost određene primjene UI-ja općenito trebalo razmatrati s obzirom na moguće posljedice, odnosno postojanje ozbiljnih rizika u okviru sektora i predviđene primjene, osobito s gledišta zaštite sigurnosti te potrošačkih i temeljnih prava. Konkretnije, primjenu UI-ja trebalo bi smatrati visokorizičnom ako ispunjava sljedeća dva kumulativna kriterija:

- prvo, da je riječ o primjeni u sektoru u kojem se, zbog karakteristika tipičnih aktivnosti u njemu, može očekivati nastanak ozbiljnih rizika. Tim se kriterijem regulatorna intervencija usmjerava prema područjima u kojima se, općenito govoreći, rizici smatraju najvjerojatnijima. Te bi sektore trebalo konkretno i iscrpno navesti u novom regulatornom okviru. Primjerice, zdravstvena skrb, promet, energetika i dijelovi javnog sektora[50]. Popis bi trebalo periodično ažurirati i prema potrebi mijenjati u skladu s relevantnim praktičnim spoznajama;
- drugo, da je način primjene u dotičnom sektoru takav da je pojava ozbiljnih rizika vjerojatna. Drugi kriterij odražava činjenicu da ne moraju sve primjene UI-ja u odabranim sektorima uzrokovati ozbiljne rizike. Primjerice, premda zdravstvena skrb općenito može biti itekako relevantan sektor, rizici od pogreške u bolničkom sustavu za naručivanje pacijenata obično nisu tako ozbiljni da bi opravdali zakonodavnu intervenciju. Rizičnost pojedine primjene mogla bi se procijeniti prema utjecaju na uključene strane. Primjerice, ima li primjena UI rješenja pravne ili slično važne učinke na prava osobe ili poduzeća, nosi li rizik od ozljede, smrti ili znatne materijalne ili nematerijalne štete, stvara li učinke koje osobe ili pravni subjekti ne mogu razumno izbjeći.

Upotrebom tih dvaju kumulativnih kriterija zajamčilo bi se da se regulatorni okvir primjenjuje ciljano i da pruža pravnu sigurnost. Obvezni zahtjevi u novom regulatornom okviru za umjetnu inteligenciju (vidjeti odjeljak D u nastavku) u načelu bi se primjenjivali samo na one primjene koje su identificirane kao visokorizične na temelju tih kumulativnih kriterija.

Ne dovodeći u pitanje prethodno navedeno, mogući su i iznimni slučajevi u kojima bi, zbog prisutnih rizika, upotrebe UI rješenja za određene svrhe trebalo smatrati same po sebi visokorizičnima, dakle

[48] Primjerice, mnogo je pravnih implikacija i sigurnosnih pitanja povezanih sa UI sustavima koji pružaju specijalizirane informacije liječnicima, sustavima koji pružaju medicinske informacije izravno pacijentu te sustavima koji sami obavljaju medicinske zahvate izravno na pacijentu. Komisija razmatra te aspekte sigurnosti i odgovornosti specifične za područje zdravstvene skrbi.

[49] Ovisno o području, primjerice u području sigurnosti proizvoda, „rizici" u zakonodavstvu EU-a mogu biti kategorizirani drukčije nego što je ovdje opisano.

[50] U javnom bi se sektoru mogla obuhvatiti područja kao što su azil, migracije, granične kontrole, pravosudne službe, službe za zapošljavanje i službe socijalne sigurnosti.

neovisno o predmetnom sektoru, i u kojima bi se i dalje primjenjivali zahtjevi navedeni u nastavku[51]. Dva moguća konkretna primjera za ilustraciju:

- s obzirom na njezinu važnost za pojedince i na pravnu stečevinu EU-a o jednakosti pri zapošljavanju, primjene UI-a u postupcima zapošljavanja i u situacijama u kojima su u pitanju radnička prava uvijek bi se smatrale visokorizičnima i stoga bi uvijek vrijedili zahtjevi u nastavku; mogle bi se razmotriti i druge specifične primjene koje utječu na prava potrošača,

- primjena UI-a za potrebe daljinske biometrijske identifikacije[52] i drugih intruzivnih tehnologija za praćenje uvijek bi se smatrala visokorizičnom i stoga bi uvijek vrijedili zahtjevi u nastavku.

D. VRSTE ZAHTJEVA

Pri izradi budućeg regulatornog okvira za UI bit će potrebno odlučiti koje će se vrste obveznih pravnih zahtjeva propisati za relevantne dionike. Te se zahtjeve može dodatno specificirati u standardima. Kako je navedeno u odjeljku C i povrh postojećeg zakonodavstva, zahtjevi bi vrijedili samo za visokorizične primjene UI-ja, čime bi se osiguralo da je svaka regulatorna intervencija usmjerena i proporcionalna.

Uzimajući u obzir smjernice stručne skupine na visokoj razini i sve dosad rečeno, zahtjevi u pogledu visokorizične primjene UI-ja mogli bi se sastojati od sljedećih ključnih elemenata, podrobnije objašnjenih u pododjeljcima u nastavku:

- podataka za učenje,
- čuvanja podataka i vođenja evidencija,
- informacija koje se pružaju,
- stabilnosti i točnosti,
- ljudskog nadzora,
- posebnih zahtjeva za određene specifične primjene UI-ja, primjerice za potrebe daljinske biometrijske identifikacije.

Radi pravne sigurnosti ti će zahtjevi biti dodatno specificirani kako bi dionici koji ih moraju ispunjavati imali jasne referentne vrijednosti.

a) Podaci za učenje

Promicanje, jačanje i obrana vrijednosti i pravila EU-a, osobito prava građana koja proizlaze iz propisa EU-a, važniji su nego ikad prije. Te se aktivnosti nedvojbeno odnose i na predmetna visokorizična UI rješenja koja se stavljaju na tržište EU-a i upotrebljavaju u njemu.

Kako je već rečeno, umjetne inteligencije nema bez podataka. Funkcioniranje mnogih UI sustava te radnje i odluke koje iz toga mogu proizići uvelike ovise o skupu podataka upotrijebljenom za učenje sustava. Zato bi trebalo poduzeti mjere kojima će se zajamčiti da su skupovi podataka za učenje UI sustava u skladu s vrijednostima i pravilima EU-a, osobito onima u pogledu sigurnosti i postojećih

[51] Važno je naglasiti da mogu važiti i drugi propisi EU-a. Primjerice, ako je dio potrošačkog proizvoda, na sigurnost UI-ja može se primjenjivati Direktiva o općoj sigurnosti proizvoda.

[52] Daljinsku biometrijsku identifikaciju trebalo bi razlikovati od biometrijske autentikacije (potonja je sigurnosni postupak za potvrdu identiteta osobe koji se oslanja na njezina jedinstvena biološka obilježja). Daljinska biometrijska identifikacija je kontinuirano daljinsko utvrđivanje identiteta više osoba u javnom prostoru usporedbom biometrijskih identifikatora (otisci prstiju, prepoznavanje lica, skeniranje rožnice, provjera vena itd.) s podacima pohranjenima u bazi podataka.

propisa za zaštitu temeljnih prava. Za skupove podataka za učenje UI sustava mogli bi se predvidjeti sljedeći zahtjevi:

- zahtjevi kojima se želi razumno zajamčiti da je nakon učenja upotreba proizvoda ili usluga omogućenih UI-jem sigurna u smislu da odgovara standardima utvrđenima u relevantnim sigurnosnim propisima EU-a (postojećima i mogućim dopunskima). To su, primjerice, zahtjevi da UI sustavi uče iz skupova podataka koji su dovoljno opsežni i pokrivaju sve relevantne scenarije kako bi se izbjegle opasne situacije;

- zahtjevi za poduzimanje razumnih mjera kojima se želi spriječiti da se, nakon učenja, upotrebom UI sustava dobivaju rezultati zbog kojih bi nastala zabranjena diskriminacija. Ti bi zahtjevi konkretno mogli sadržavati obveze da se upotrebljavaju skupovi podataka dovoljne reprezentativnosti, ponajprije s obzirom na odgovarajuću zastupljenost svih relevantnih dimenzija spola, etničke pripadnosti i drugih mogućih temelja zabranjene diskriminacije;

- zahtjevi u cilju primjerene zaštite privatnosti i osobnih podataka tijekom služenja proizvodima i uslugama temeljenima na UI-ju. Opća uredba o zaštiti podataka i Direktiva o zaštiti podataka pri izvršavanju zakonodavstva primjenjuju se ako je riječ o pitanju koje je obuhvaćeno njihovim područjima primjene.

b) Vođenje evidencija i čuvanje podataka

Zbog elemenata kao što su složenost i netransparentnost mnogih UI sustava te s njima povezanih mogućih problema pri učinkovitoj provjeri sukladnosti s važećim pravilima i provedbi tih pravila, potrebni su zahtjevi u pogledu vođenja evidencija o programiranju algoritama i podacima upotrijebljenima za učenje visokorizičnih UI sustava te, u određenim slučajevima, u pogledu čuvanja samih podataka. Ti zahtjevi zapravo omogućuju da se potencijalno problematičnim radnjama ili odlukama UI sustava uđe u trag i da ih se provjeri. To bi trebalo ne samo olakšati nadzor i provedbu nego bi moglo i snažnije potaknuti relevantne gospodarske subjekte na uvažavanje tih pravila u ranoj fazi.

Radi toga bi se u regulatornom okviru moglo propisati da bi trebalo:

- voditi točne evidencije o skupu podataka upotrijebljenom za učenje i testiranje UI sustavâ, uključujući opis glavnih karakteristika i postupka odabira podataka,

- čuvati, u određenim opravdanim slučajevima, same skupove podataka,

- voditi dokumentaciju o metodologijama programiranja[53] i učenja te procesima i tehnikama primijenjenima za izradu, testiranje i validaciju sustavâ UI-ja; također i kad je to relevantno radi sigurnosti i izbjegavanja pristranosti koja bi mogla dovesti do zabranjene diskriminacije.

Evidencije, dokumentaciju i, prema potrebi, skupove podataka trebalo bi čuvati određeno, razumno dugo razdoblje kako bi se relevantni propisi mogli djelotvorno provoditi. Trebalo bi poduzeti mjere da budu dostupni na zahtjev, osobito za testiranje ili inspekcije nadležnih tijela. Prema potrebi trebalo bi uspostaviti mehanizme za zaštitu povjerljivih informacija kao što su poslovne tajne.

c) Pružanje informacija

[53] Primjerice, dokumentaciju algoritma s informacijama o modelu za koji se algoritam optimira, početno definiranim težinskim vrijednostima za određene parametre itd.

Transparentnost nije potrebna samo u okviru zahtjeva iz prethodne točke, koji se odnose na vođenje evidencije. Za ostvarenje zadanih ciljeva, ponajprije promicanje odgovorne upotrebe UI-ja, izgradnju povjerenja i, prema potrebi, olakšavanje pravne zaštite, važno je da se odgovarajuće informacije o korištenju visokorizičnih UI sustava pružaju unaprijed.

U skladu s tim razmotriti bi se mogli sljedeći zahtjevi:

- pružanje jasnih informacija o mogućnostima i ograničenjima UI sustavâ, osobito o njihovoj predviđenoj namjeni, uvjetima u kojima se može očekivati da će funkcionirati kako treba i očekivanoj točnosti u postizanju zadane svrhe. Te su informacije osobito važne onima koji primjenjuju sustave, ali mogu biti relevantne i nadležnim tijelima te drugim uključenim stranama;

- zasebno od toga, građani bi trebali biti jasno obaviješteni o tome da se nalaze u interakciji sa UI sustavom, a ne s čovjekom. Premda propisi EU-a o zaštiti podataka već sadržavaju određena pravila te vrste[54], za postizanje gorespomenutih ciljeva možda će biti nužni dodatni zahtjevi. U tom bi slučaju trebalo izbjeći nepotrebno opterećenje. Stoga takve informacije ne bi bile potrebne, primjerice, u situacijama u kojima je građanima smjesta očito da se nalaze u interakciji sa UI sustavima. Nadalje, važno je da dane informacije budu objektivne, jezgrovite i lako razumljive. Način davanja informacija trebao bi ovisiti o konkretnom kontekstu.

d) Stabilnost i točnost

UI sustavi i, svakako, visokorizična UI rješenja moraju biti tehnički stabilni i točni da bi bili pouzdani. To znači da se takvi sustavi moraju razvijati odgovorno i pritom se rizici koje mogu prouzročiti unaprijed moraju dobro i propisno uzeti u obzir. UI sustavi moraju biti razvijeni i funkcionirati na način koji jamči očekivanu pouzdanost rada. Trebalo bi poduzeti sve razumne mjere za smanjenje rizika od štete.

U skladu s tim razmotriti bi se mogli sljedeći elementi:

- zahtjevi kojima se osigurava stabilnost i točnost UI sustava, ili da barem vjerno odražavaju svoju točnost, u svim fazama životnog ciklusa,

- zahtjevi kojima se osigurava obnovljivost rezultata,

- zahtjevi kojima se osigurava da UI sustavi mogu primjereno odgovoriti na pogreške ili nedosljednosti u svim fazama životnog ciklusa,

- zahtjevi kojima se osigurava otpornost UI sustava na otvorene napade i skrivenije pokušaje manipulacije podacima ili samim algoritmima te da se u takvim slučajevima poduzimaju zaštitne mjere.

e) Ljudski nadzor

[54] Konkretno, na temelju članka 13. stavka 2. točke (f) Opće uredbe o zaštiti podataka voditelji obrade dužni su u trenutku prikupljanja osobnih podataka ispitanicima pružiti dodatne informacije o postojanju automatiziranog donošenja odluka i još neke informacije kako bi se osigurala poštena i transparentna obrada.

Ljudski nadzor pomaže u sprečavanju sustava umjetne inteligencije da ugrozi autonomiju čovjeka ili prouzroči druge štetne učinke. Cilj pouzdanog, etičnog i antropocentričnog UI-ja može se postići samo uz odgovarajuće sudjelovanje čovjeka u visokorizičnim primjenama UI-ja.

Premda se sve primjene UI-ja za koje se u ovoj Bijeloj knjizi razmatra primjena specifičnog pravnog režima smatraju visokorizičnima, odgovarajuća vrsta i stupanj ljudskog nadzora mogu se razlikovati od slučaja do slučaja. Konkretno, ovisit će o predviđenoj namjeni sustavâ i učincima koje bi primjena mogla imati na njome zahvaćene građane i pravne subjekte. Nadzorom se, usto, neće dovoditi u pitanje prava utvrđena Općom uredbom o zaštiti podataka u slučaju obrade osobnih podataka UI sustavom. Ljudski nadzor mogao bi imati, među ostalim, sljedeće oblike:

- rezultat UI sustava ne izvršava se dok ga čovjek ne pregleda i odobri (npr. zahtjev za socijalnu pomoć može odbiti samo čovjek),

- rezultat UI sustava izvršava se odmah, ali obvezna je naknadna ljudska intervencija (npr. UI sustav može odbiti zahtjev za kreditnu karticu, no mora postojati mogućnost da čovjek naknadno preispita tu odluku),

- praćenje rada UI sustava i mogućnost intervencije i deaktivacije u stvarnom vremenu (npr. u automobilu bez vozača postoji gumb ili postupak za prekid rada ako čovjek odluči da automobil ne radi sigurno),

- ograničavanje rada UI sustava u fazi projektiranja (npr. automobil bez vozača prestat će s radom u određenim uvjetima niske vidljivosti u kojima se može smanjiti pouzdanost senzora ili pak u svim uvjetima održavati određeni razmak od vozila ispred sebe).

f) Posebni zahtjevi za daljinsku biometrijsku identifikaciju

Prikupljanje i korištenje biometrijskih podataka[55] za potrebe daljinske identifikacije[56], primjerice sustavom za prepoznavanje lica na javnim mjestima, nosi posebne rizike za temeljna prava[57]. Utjecaj korištenja UI sustava za daljinsku biometrijsku identifikaciju na temeljna prava može se znatno razlikovati ovisno o svrsi, kontekstu i opsegu primjene.

Pravilima EU-a o zaštiti podataka u načelu se zabranjuje obrada biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, osim pod posebnim uvjetima[58]. Konkretno, prema Općoj uredbi o

[55] Biometrijski podaci definirani su kao „osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu autentikaciju ili identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci (otisci prstiju).” (članak 3. točka 13. Direktive o zaštiti podataka pri izvršavanju zakonodavstva; članak 4. točka 14. Opće uredbe o zaštiti podataka; članak 3. točka 18. Uredbe (EU) 2018/1725).

[56] Kad je riječ o prepoznavanju lica, identifikacija znači da se biometrijski uzorak izveden iz fotografije lica osobe uspoređuje s mnogim drugim uzorcima pohranjenima u bazi podataka kako bi se provjerilo je li u njoj pohranjena njezina slika. Autentikacija (ili verifikacija) se pak često naziva poklapanjem jedan na jedan. Ona omogućuje usporedbu dvaju biometrijskih uzoraka za koje se obično pretpostavlja da pripadaju istoj osobi. Dva se uzorka uspoređuju kako bi se utvrdilo je li na slikama ista osoba. Takav se postupak primjenjuje, primjerice, na vratima automatske granične kontrole na aerodromima.

[57] Na primjer, na ljudsko dostojanstvo. S tim u vezi, kad je riječ o temeljnim pravima u kontekstu tehnologije prepoznavanja lica, najspornije je pitanje pravâ na poštovanje privatnog života i zaštitu osobnih podataka. Postoji i mogućnost utjecaja na nediskriminaciju i prava posebnih skupina kao što su djeca, starije osobe i osobe s invaliditetom. Usto, primjena te tehnologije ne smije ugroziti slobodu izražavanja, udruživanja i okupljanja. Vidjeti: Tehnologija prepoznavanja lica: pitanje temeljnih prava u kontekstu provedbe zakona, https://fra.europa.eu/en/publication/2019/facial-recognition.

[58] Članak 9. Opće uredbe o zaštiti podataka, članak 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva. Vidjeti i članak 10. Uredbe (EU) 2018/1725 (primjenjuje se na institucije i tijela EU-a).

zaštiti podataka takva se obrada može provoditi samo na temelju ograničenog broja razloga, među kojima je značajni javni interes najvažniji. U tom se slučaju obrada mora temeljiti na pravu Unije ili nacionalnom pravu koje je proporcionalno i kojim se poštuje bit prava na zaštitu podataka i propisuju odgovarajuće zaštitne mjere. Prema Direktivi o zaštiti podataka pri izvršavanju zakonodavstva takva obrada mora biti strogo nužna, u načelu odobrena na temelju prava EU-a ili nacionalnog prava, i na nju se moraju primjenjivati odgovarajuće zaštitne mjere. Budući da je zabranjena pravom EU-a, bilo kakva obrada biometrijskih podataka za potrebe jedinstvene identifikacije fizičke osobe bila bi iznimka od te zabrane i za nju bi vrijedila Povelja EU-a o temeljnim pravima.

Iz toga proizlazi, u skladu s postojećim pravilima EU-a o zaštiti podataka i Poveljom o temeljnim pravima, da se UI može primjenjivati za potrebe daljinske biometrijske identifikacije ako je takva primjena propisno opravdana, proporcionalna i podložna odgovarajućim zaštitnim mjerama.

Kako bi se uklonile sumnje koje bi primjena UI-ja u takve svrhe na javnim mjestima mogla izazvati u društvu i izbjegla fragmentacija unutarnjeg tržišta, Komisija će pokrenuti opsežnu europsku raspravu o specifičnim okolnostima, ako postoje, koje bi mogle opravdati takvu primjenu i o zajedničkim zaštitnim mjerama.

E. ADRESATI

Kad je riječ o adresatima pravnih zahtjeva koji bi se primjenjivali na prethodno navedene visokorizične primjene UI-ja, valja razmotriti dva glavna pitanja.

Prvo je pitanje raspodjele obveza među uključenim gospodarskim subjektima. U životnom ciklusu UI sustava sudjeluje mnogo dionika. Među njima su razvojni programeri, subjekti koji primjenjuju proizvode ili usluge s UI-jem te drugi potencijalni dionici (proizvođač, distributer ili uvoznik, pružatelj usluge, profesionalni ili privatni korisnik).

Komisija smatra da bi u budućem regulatornom okviru svaku obvezu trebalo propisati dionicima koji su u najboljem položaju za smanjenje potencijalnih rizika. Primjerice, programeri koji razvijaju UI možda su u najboljem položaju da smanje rizike koji mogu nastati u razvojnoj fazi, no u fazi primjene mogli bi imati ograničenu mogućnost kontrole rizika. U tom bi se slučaju razvojnom programeru trebala propisati odgovarajuća obveza. Time se ne prejudicira koja bi strana, za potrebe odgovornosti prema krajnjim korisnicima ili drugim oštećenim stranama i učinkovitog pristupa pravosuđu, trebala biti odgovorna za eventualnu štetu. Propisima EU-a o odgovornosti za proizvode odgovornost za neispravne proizvode pripisuje se proizvođaču, ne dovodeći u pitanje nacionalne zakone koji mogu dopuštati odštetu i od drugih strana.

Drugo je pitanje zemljopisnog opsega zakonodavne intervencije. Komisija smatra da je presudno da se zahtjevi primjenjuju na sve relevantne gospodarske subjekte koji u EU-u pružaju proizvode ili usluge temeljene na UI-ju, bez obzira na to je li im poslovni nastan u EU-u. U protivnom se navedeni ciljevi zakonodavne intervencije možda neće moći u cijelosti ostvariti.

F. POŠTOVANJE I PROVEDBA PROPISA

Kako bi umjetna inteligencija bila pouzdana, sigurna i u skladu s europskim vrijednostima i pravilima, nadležna nacionalna i europska tijela te uključene strane moraju poštovati važeće pravne zahtjeve u praksi i učinkovito ih provoditi. Nadležna tijela trebala bi biti u mogućnosti istražiti pojedinačne slučajeve, ali i procijeniti utjecaj na društvo.

S obzirom na visoku rizičnost određenih primjena UI-ja za građane i naše društvo (vidjeti odjeljak A), Komisija smatra da bi u ovoj fazi za provjeru i osiguravanje poštovanja pojedinih navedenih obveznih

zahtjeva za visokorizične primjene (vidjeti odjeljak D) bilo potrebno prethodno objektivno ocjenjivanje sukladnosti. To bi ocjenjivanje moglo uključivati postupke za testiranje, inspekciju ili certifikaciju [59]. Moglo bi također obuhvaćati provjere algoritama i skupova podataka koji se upotrebljavaju u razvojnoj fazi.

Ocjenjivanje sukladnosti za visokorizične primjene UI-ja trebalo bi ugraditi u mehanizme ocjenjivanja sukladnosti koji već postoje za velik broj proizvoda koji se stavljaju na unutarnje tržište EU-a. Ako se nije moguće osloniti na takve postojeće mehanizme, možda će biti potrebno uspostaviti slične mehanizme na temelju najboljih primjera iz prakse i mogućeg doprinosa dionika i europskih organizacija za normizaciju. Svaki bi takav novi mehanizam trebao biti proporcionalan i nediskriminatoran te imati transparentne i objektivne kriterije u skladu s međunarodnim obvezama.

Pri izradi i uvođenju sustava na temelju prethodne ocjene sukladnosti osobito bi trebalo voditi računa o sljedećem:

- gore navedeni zahtjevi nisu nužno primjereni za provjeru prethodnim ocjenjivanjem sukladnosti. Primjerice, zahtjev u pogledu pružanja informacija općenito nije osobito prikladan za provjeru takvim ocjenjivanjem;

- određeni UI sustavi imaju mogućnost razvoja i učenja na temelju iskustva, pa tijekom njihova životnog ciklusa može biti potrebno ponavljati ocjenjivanje,

- postoji potreba da se provjere podaci koji služe za učenje te relevantne metodologije programiranja i učenja, procesi i tehnike upotrijebljeni za izradu, testiranje i validaciju UI sustava,

- u slučaju da ocjenjivanje sukladnosti pokaže da UI sustav ne ispunjava zahtjeve, primjerice u pogledu podataka upotrijebljenih za njegovo učenje, uočeni će se nedostaci morati ispraviti, na primjer ponovnim učenjem sustava u EU-u na način koji jamči ispunjenje svih primjenjivih zahtjeva.

Ocjenjivanje sukladnosti bilo bi obvezno za sve gospodarske subjekte na koje se zahtjevi odnose, bez obzira na to gdje im je poslovni nastan[60]. Kako bi se ograničilo opterećenje MSP-ova, može se predvidjeti određena potporna struktura, među ostalim u okviru digitalnoinovacijskih centara. Usto, postizanje sukladnosti moglo bi se olakšati standardima i namjenskim internetskim alatima.

Prethodnim ocjenjivanjem sukladnosti ne bi se trebali dovoditi u pitanje praćenje sukladnosti i *ex post* provedba u nadležnosti nacionalnih tijela. To ne vrijedi samo za visokorizične primjene nego i za druge primjene UI-ja koje podliježu pravnim zahtjevima, premda bi nadležna nacionalna tijela veću pozornost mogla pridavati prvima zbog njihove visokorizične prirode. Za *ex post* kontrole relevantna bi primjena UI-ja trebala biti primjereno dokumentirana (vidjeti odjeljak E) i, prema potrebi, trebala bi postojati mogućnost da treće strane kao što su nadležna tijela testiraju takve primjene. To može biti posebno važno ako se pojave rizici za temeljna prava koji ovise o kontekstu. Takvo praćenje

[59] Sustav bi se temeljio na postupcima ocjenjivanja sukladnosti u EU-u, vidjeti Odluku 768/2008/EZ ili Uredbu (EU) 2019/881 (Akt o kibersigurnosti), uzimajući u obzir posebnosti UI-ja. Vidjeti Plavi vodič o provedbi pravila EU-a o proizvodima, 2014.

[60] O relevantnoj strukturi upravljanja, uključujući tijela imenovana za provedbu ocjenjivanja sukladnosti, govori se u odjeljku H.

sukladnosti trebalo bi biti dio programa kontinuiranog nadzora tržišta. O aspektima povezanima s upravljanjem još se govori u odjeljku H.

Povrh toga, i za visokorizične i za druge primjene UI-ja trebalo bi osigurati djelotvornu sudsku zaštitu strana na koje su UI sustavi štetno utjecali. Pitanja odgovornosti dodatno se razmatraju u Izvješću o okviru za sigurnost i odgovornost priloženom ovoj Bijeloj knjizi.

G. DOBROVOLJNO OZNAČIVANJE PRIMJENA UMJETNE INTELIGENCIJE KOJE NISU VISOKORIZIČNE

Za primjene UI-ja koje se ne smatraju „visokorizičnima" (vidjeti odjeljak C) i koje stoga ne podliježu obveznim zahtjevima (vidjeti odjeljke D, E i F) opcija bi mogla biti, uz važeće zakonodavstvo, uspostava programa dobrovoljnog označivanja.

Prema tom programu zainteresirani gospodarski subjekti koji nisu obuhvaćeni obveznim zahtjevima mogli bi, na dobrovoljnoj osnovi, odlučiti da se na njih primjenjuju ti zahtjevi ili poseban skup sličnih zahtjeva utvrđenih samo za potrebe dobrovoljnog programa. Dotičnim gospodarskim subjektima zatim bi se dodijelila oznaka kvalitete za njihove primjene UI-ja.

Tu bi oznaku kvalitete gospodarski subjekti mogli koristiti kao znak pouzdanosti svojih proizvoda i usluga temeljenih na UI-ju. Korisnici bi zahvaljujući tome mogli lako prepoznati da su konkretni proizvodi i usluge u skladu s određenim objektivnim i standardiziranim mjerilima na razini EU-a koja nadilaze redovno primjenjive pravne obveze. To bi pridonijelo izgradnji povjerenja korisnika u UI sustave i potaknulo opću primjenu te tehnologije.

Ta bi mogućnost podrazumijevala izradu novog pravnog instrumenta kojim se utvrđuje okvir za dobrovoljno označivanje za razvojne programere i/ili subjekte koji primjenjuju UI sustave koji se ne smatraju visokorizičnima. Premda bi sudjelovanje u programu bilo dobrovoljno, zahtjevi bi bili obvezujući nakon što se razvojni programer ili subjekt odluči koristiti oznaku. Kako bi se osiguralo da se poštuju svi zahtjevi, nužna bi bila kombinacija *ex ante* i *ex post* provedbenih mjera.

H. UPRAVLJANJE

Kako bi se izbjegla rascjepkanost odgovornosti, povećali kapaciteti u državama članicama i osiguralo da se Europa postupno opremi kapacitetima potrebnima za testiranje i certifikaciju proizvoda i usluga temeljenih na UI-ju, potrebna je europska upravljačka struktura za umjetnu inteligenciju u obliku okvira za suradnju nacionalnih nadležnih tijela. U tom bi kontekstu bilo korisno pružiti potporu nadležnim nacionalnim tijelima kako bi im se omogućilo da iskoriste svoje ovlasti u pogledu UI-ja.

Europska upravljačka struktura mogla bi imati razne zadaće, od foruma za redovitu razmjenu informacija i najboljih rješenja iz prakse do identificiranja perspektivnih trendova i savjetovanja o standardizaciji i certifikaciji. Trebala bi imati i ključnu ulogu u olakšavanju provedbe pravnog okvira, na primjer davanjem smjernica, mišljenja i stručnih savjeta. Radi toga bi se trebala oslanjati na mrežu nacionalnih tijela kao i na sektorske mreže i regulatorna tijela, na nacionalnoj razini i razini EU-a. Usto, Komisiji bi mogao pomagati stručni odbor.

Upravljačka struktura trebala bi omogućivati maksimalno sudjelovanje dionika. S dionicima – udrugama potrošača i socijalnim partnerima, poduzećima, znanstvenicima i organizacijama civilnog društva – trebalo bi se savjetovati o provedbi i daljnjem razvoju okvira.

U predloženoj upravljačkoj strukturi ne bi trebalo podvostručavati postojeće funkcije u strukturama uspostavljenima u područjima financija, farmaceutskih proizvoda, zračnog prometa, medicinskih uređaja, zaštite potrošača i zaštite podataka. Umjesto toga trebalo bi uspostaviti bliske veze s drugim nadležnim tijelima, nacionalnima i na razini EU-a, u raznim sektorima kako bi se upotpunilo sadašnje

stručno znanje i pomoglo postojećim tijelima u praćenju i nadzoru aktivnosti gospodarskih subjekata koji primjenjuju UI sustave ili nude proizvode i usluge temeljene na UI-ju.

Naposljetku, bude li se ta opcija realizirala, ocjenjivanje sukladnosti moglo bi se povjeriti prijavljenim tijelima koja su imenovale države članice. Centri za testiranje trebali bi omogućiti neovisnu reviziju i ocjenjivanje UI sustava u skladu s opisanim zahtjevima. Neovisno ocjenjivanje povećat će povjerenje i osigurati objektivnost te možda olakšati rad relevantnih nadležnih tijela.

EU ima izvrsne centre za testiranje i ocjenjivanje i svoje bi kapacitete trebao povećavati i u području umjetne inteligencije. Gospodarski subjekti s poslovnim nastanom u trećim zemljama koji žele ući na unutarnje tržište mogli bi se obratiti imenovanim tijelima u EU-u ili, ovisno o sporazumima o uzajamnom priznavanju s trećim zemljama, tijelima iz treće zemlje imenovanima za provedbu takvog ocjenjivanja.

Upravljačka struktura koja se odnosi na UI i moguća ocjenjivanja sukladnosti o kojima je ovdje riječ ne bi utjecala na ovlasti i odgovornosti koje relevantna nadležna tijela imaju u pojedinim sektorima ili u pojedinim pitanjima na temelju postojećeg prava EU-a.

6. ZAKLJUČAK

Umjetna inteligencija strateška je tehnologija koja nudi mnoge koristi građanima, poduzećima i društvu u cjelini, pod uvjetom da je antropocentrična, etična, održiva i da poštuje temeljna prava i vrijednosti. Umjetna inteligencija omogućuje važan porast učinkovitosti i produktivnosti koji može povećati konkurentnost europske industrije i dobrobit građana. Može pomoći i u rješavanju gorućih društvenih problema. To obuhvaća i borbu protiv klimatskih promjena i uništavanja okoliša, probleme povezane s održivošću i demografskim promjenama, zaštitu naših demokracija i, prema potrebi i proporcionalno svrsi, borbu protiv kriminala.

Ako želi potpuno iskoristiti mogućnosti koje nudi umjetna inteligencija, Europa mora razviti i povećati potrebne industrijske i tehnološke kapacitete. Kako je navedeno u pratećoj europskoj strategiji za podatke, za to su potrebne i mjere koje će EU-u omogućiti da postane svjetski predvodnik u području podataka.

Cilj je europskog pristupa promicati inovacijski kapacitet Europe u području umjetne inteligencije i ujedno podupirati razvoj i primjenu etične i pouzdane umjetne inteligencije u cijelom gospodarstvu EU-a. Umjetna inteligencija trebala bi služiti građanima i biti snaga koja će unaprijediti društvo.

Ovom Bijelom knjigom i pratećim Izvješćem o okviru za sigurnost i odgovornost Komisija pokreće opsežno savjetovanje s državama članicama, civilnim društvom, industrijom i akademskom zajednicom o konkretnim prijedlozima za europski pristup umjetnoj inteligenciji. Ti se prijedlozi, s jedne strane, odnose na instrumente politike za poticanje ulaganja u istraživanja i inovacije, poboljšanje razvoja vještina i poticanje primjene umjetne inteligencije među MSP-ovima te, s druge strane, na prijedloge ključnih elemenata budućeg regulatornog okvira. Savjetovanje će omogućiti sveobuhvatan dijalog sa svim zainteresiranim stranama na temelju kojeg će Komisija odlučiti o daljnjim koracima.

Komisija poziva da komentare o prijedlozima iz Bijele knjige iznesete u otvorenom javnom savjetovanju na adresi https://ec.europa.eu/info/consultations_en. Komentari se primaju do 19. svibnja 2020.

Uobičajena je praksa Komisije da se podnesci primljeni u okviru javnog savjetovanja objavljuju. Moguće je, međutim, zatražiti da podnesci ili njihovi dijelovi ostanu povjerljivi. U tom slučaju na prvoj stranici podneska jasno navedite da ga se ne smije objaviti te pošaljite i primjerak podneska koji nije povjerljiv i koji Komisija može objaviti.