EDPB-EDPS

Zajedničko mišljenje 5/2021

o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji)

18. lipnja 2021.

Sažetak

Dana 21. travnja 2021. Europska komisija predstavila je svoj Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (dalje u tekstu: Prijedlog). Europski odbor za zaštitu podataka (EDPB) i Europski nadzornik za zaštitu podataka (EDPS) pozdravljaju zabrinutost zakonodavca u pogledu uporabe umjetne inteligencije (UI) u Europskoj uniji (EU) i ističu da Prijedlog ima vrlo važne **implikacije za zaštitu podataka**.

EDPB i EDPS napominju da je **pravna osnova** Prijedloga prvenstveno članak 114. Ugovora o funkcioniranju Europske unije (UFEU). Osim toga, Prijedlog se temelji i na članku 16. UFEU-a jer sadržava određena posebna pravila o zaštiti pojedinaca u pogledu obrade osobnih podataka, prije svega ograničenja uporabe sustavâ umjetne inteligencije za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona. EDPB i EDPS podsjećaju da, sukladno sudskoj praksi Suda Europske unije (Sud), članak 16. UFEU-a predstavlja odgovarajuću pravnu osnovu kad je zaštita osobnih podataka jedan od ciljeva ili bitnih sastavnica pravila koje je donio zakonodavac Unije. Primjena članka 16. UFEU-a podrazumijeva i **potrebu za osiguranjem neovisnog nadzora za potrebe usklađenosti** sa zahtjevima koji se odnose na obradu osobnih podataka, što je propisano i člankom 8. Povelje Europske unije o temeljnim pravima.

Što se tiče **područja primjene Prijedloga**, EDPB i EDPS pozdravljaju činjenicu da on obuhvaća stavljanje na raspolaganje i uporabu sustavâ umjetne inteligencije u institucijama, tijelima ili agencijama EU-a. Međutim, činjenica da je **međunarodna suradnja u području izvršavanja zakonodavstva isključena iz područja primjene** Prijedloga izaziva ozbiljnu zabrinutost EDPB-a i EDPS-a jer se takvim isključenjem stvara značajan rizik od zaobilaženja propisa (npr. u trećim zemljama ili međunarodnim organizacijama koje se koriste visokorizičnim aplikacijama na koje se oslanjaju javna tijela u EU-u).

EDPB i EDPS pozdravljaju **pristup temeljen na riziku**, koji je primijenjen pri izradi Prijedloga. Međutim, budući da se Prijedlog odnosi na aspekte povezane sa zaštitom osobnih podataka, taj bi pristup trebao biti pojašnjen, a načelo „rizika za temeljna prava" treba biti usklađeno s Općom uredbom o zaštiti podataka (GDPR) i Uredbom (EU) 2018/1725 (Europska uredba o zaštiti podataka – EUDPR).

EDPB i EDPS slažu se s dijelom Prijedloga u kojem se navodi da klasifikacija **nekog sustava umjetne inteligencije kao visokorizičnog ne podrazumijeva nužno da je on sam po sebi zakonit** i da se korisnik njime može koristiti kao takvim. Voditelj obrade **možda će morati ispuniti dodatne zahtjeve koji proizlaze iz zakonodavstva EU-a u području zaštite podataka.** Nadalje, usklađenost s pravnim obvezama koje proizlaze iz zakonodavstva Unije (uključujući u području zaštite osobnih podataka) treba biti preduvjet za uvrštenje proizvoda na europsko tržište kao proizvoda s oznakom CE. U tu svrhu EDPB i EDPS smatraju da bi u **glavu III. poglavlje 2. trebalo uvrstiti zahtjev za osiguranje usklađenosti s Općom uredbom o zaštiti podataka i Europskom uredbom o zaštiti podataka**. Osim toga, EDPB i EDPS smatraju da je postupak ocjenjivanja sukladnosti sadržan u Prijedlogu potrebno prilagoditi na način da treće strane uvijek provode *ex ante* procjene sukladnosti visokorizičnih sustava umjetne inteligencije.

S obzirom na visok rizik od diskriminacije, Prijedlogom je zabranjeno „društveno vrednovanje" koje se provodi ‚u određenom razdoblju' ili koje provode ‚tijela javne vlasti' ili koje se provodi ‚u njihovo ime'. Međutim, privatna društva, kao što su pružatelji usluga društvenih mreža ili pružatelji usluga u oblaku, također mogu obrađivati goleme količine osobnih podataka i provoditi društveno vrednovanje. Zbog toga bi **budućom Uredbom o umjetnoj inteligenciji trebali biti zabranjeni svi oblici društvenog vrednovanja**.

Daljinska biometrijska identifikacija pojedinaca na javnim mjestima predstavlja značajan rizik od zadiranja u privatni život pojedinaca, što ima ozbiljne posljedice na očekivanje stanovništva da će biti anonimno na javnim mjestima. Zbog toga EDPB i EDPS **pozivaju na opću zabranu svih oblika uporabe umjetne inteligencije za automatizirano prepoznavanje ljudskih obilježja na javnim mjestima**, kao što su prepoznavanje lica, ali i načina kretanja, otisaka prstiju, DNK-a, glasa, načina tipkanja i drugih biometrijskih ili bihevioralnih signala, u svakom kontekstu. Isto tako, preporučuje se **zabrana sustava umjetne inteligencije kojima se pojedinci razvrstavaju u skupine** na temelju etničke pripadnosti, roda, kao i političke ili seksualne orijentacije ili drugih osnova na temelju kojih je zabranjena diskriminacija u skladu s člankom 21. Povelje. Nadalje, EDPB i EDPS smatraju da je uporaba umjetne inteligencije za **izvođenje zaključaka o emocijama pojedinaca vrlo nepoželjna i da je treba zabraniti**.

EDPB i EDPS pozdravljaju **činjenicu da je EDPS imenovan nadležnim tijelom i tijelom za nadzor tržišta koje će provoditi nadzor nad institucijama, agencijama i tijelima EU-a**. Međutim, trebalo bi dodatno pojasniti ulogu i zadaće EDPS-a, osobito kad je riječ o njegovoj ulozi tijela za nadzor tržišta. Nadalje, budućom Uredbom o umjetnoj inteligenciji trebala bi biti jasno utvrđena **neovisnost nadzornih tijela** u provedbi zadaća nadzora i provedbe.

Imenovanjem tijelâ za zaštitu podataka nacionalnim nadzornim tijelima zajamčio bi se usklađeniji regulatorni pristup i pridonijelo bi se dosljednom tumačenju odredbi o obradi podataka te bi se izbjegle proturječnosti u njihovoj provedbi među državama članicama. Zbog toga EDPB i EDPS **smatraju da bi tijela za zaštitu podataka trebala biti imenovana nacionalnim nadzornim tijelima u skladu s člankom 59. Prijedloga.**

Komisiji je Prijedlogom dodijeljena glavna uloga u „Europskom odboru za umjetnu inteligenciju" (EAIB). Takva je uloga protivna potrebi da europsko tijelo za umjetnu inteligenciju bude neovisno o bilo kakvom političkom utjecaju. Kako bi se zajamčila njegova neovisnost, budućom Uredbom o umjetnoj inteligenciji trebala bi biti predviđena **veća samostalnost EAIB-a** i trebalo bi biti zajamčeno da on može samoinicijativno djelovati.

S obzirom na širenje sustavâ umjetne inteligencije na cijelom području jedinstvenog tržišta i vjerojatnost prekograničnih slučajeva, postoji velika potreba za usklađenom provedbom i pravilnom dodjelom ovlasti nacionalnih nadzornih tijela. EDPB i EDPS predlažu da se predvidi **mehanizam kojim će se osigurati jedinstvena kontaktna točka za pojedince na koje se primjenjuje zakonodavstvo, kao i za poduzeća, za svaki sustav umjetne inteligencije.**

Što se tiče **izoliranih okruženja**, EDPB i EDPS **preporučuju pojašnjenje njihova opsega i ciljeva**. Prijedlogom bi također trebalo biti jasno navedeno da bi pravna osnova takvih izoliranih okruženja trebala biti usklađena sa zahtjevima utvrđenima postojećim okvirom za zaštitu podataka.

Sustavu certifikacije navedenom u Prijedlogu **nedostaje jasna poveznica sa zakonodavstvom EU-a u području zaštite podataka**, kao i s ostalim zakonodavstvom EU-a i država članica primjenjivim na svako „područje" visokorizičnog sustava umjetne inteligencije te njime nisu uzeta u obzir **načela smanjenja**

količine podataka i tehničke zaštite podataka kao jedan od aspekata koje valja razmotriti **prije ishođenja oznake CE**. Stoga EDPB i EDPS predlažu da se Prijedlog izmjeni na način da se pojasni odnos između potvrda izdanih u skladu s navedenom Uredbom i mehanizama certificiranja, pečata i oznaka za zaštitu podataka. Konačno, tijela za zaštitu podataka trebala bi sudjelovati u pripremi i uspostavi usklađenih normi i zajedničkih specifikacija.

Što se tiče **kodeksâ ponašanja**, EDPB i EDPS smatraju da je **potrebno pojasniti** treba li zaštitu osobnih podataka smatrati jednim od „dodatnih zahtjeva" na koje se ti kodeksi ponašanja mogu odnositi te zajamčiti da „tehničke specifikacije i rješenja" nisu protivni pravilima i načelima postojećeg okvira EU-a za zaštitu podataka.

SADRŽAJ

1 UVOD....6
2 ANALIZA KLJUČNIH NAČELA PRIJEDLOGA....8
2.1 Područje primjene Prijedloga i njegov odnos s postojećim pravnim okvirom....8
2.2 Pristup koji se temelji na riziku....9
2.3 Zabranjene primjene umjetne inteligencije....11
2.4 Visokorizični sustavi umjetne inteligencije....14
2.4.1 Potreba za *ex ante* ocjenjivanjem sukladnosti koje provode vanjske treće strane....14
2.4.2 Područje primjene uredbe također mora obuhvaćati sustave umjetne inteligencije koji se već koriste....14
2.5 Upravljanje i Europski odbor za umjetnu inteligenciju....15
2.5.1 Upravljanje....15
2.5.2 Europski odbor za umjetnu inteligenciju....17
3 INTERAKCIJA s okvirom za zaštitu podataka....18
3.1 Odnos Prijedloga i postojećeg prava EU-a u području zaštite podataka....18
3.2 Izolirana okruženja i daljnja obrada (članci 53. i 54. Prijedloga)....19
3.3 Transparentnost....21
3.4 Obrada posebnih kategorija podataka i podaci povezani s kaznenim djelima....21
3.5 Mehanizmi za postizanje usklađenosti....22
3.5.1 Certifikacija....22
3.5.2 Kodeksi ponašanja....23
4 ZAKLJUČAK....24

Europski odbor za zaštitu podataka i Europski nadzornik za zaštitu podataka

Uzimajući u obzir članak 42. stavak 2. Uredbe (EU) 2018/1725 od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ[1],

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.[2],

uzimajući u obzir zahtjev za zajedničko mišljenje EDPS-a i EDPB-a od 22. travnja 2021. o Prijedlogu uredbe o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji),

USVOJILI SU SLJEDEĆE ZAJEDNIČKO MIŠLJENJE

1 UVOD

1. Pojava sustavâ umjetne inteligencije (UI) vrlo je važan korak u razvoju tehnologija i načinu na koji ljudi djeluju u interakciji s njima. Umjetna inteligencija skup je ključnih tehnologija koje će dubinski izmijeniti naše svakodnevne živote, u društvenom ili ekonomskom smislu. Tijekom narednih nekoliko godina očekuje se donošenje odluka od presudne važnosti za umjetnu inteligenciju, koji će nam pomagati u svladavanju nekih od najvećih izazova s kojima se danas suočavamo u brojnim područjima, od zdravlja do mobilnosti, ili od javne uprave do obrazovanja.

2. Međutim, taj obećani napredak ne dolazi bez rizika. Budući da su učinci sustava umjetne inteligencije na pojedince i društvo u velikoj mjeri nepoznati, rizici su vrlo relevantni. Stvaranje sadržaja, donošenje predviđanja ili odluke na automatizirani način, kako to čine sustavi umjetne inteligencije, s pomoću tehnika strojnog učenja ili logičkih i probabilističkih pravila donošenja zaključaka, nisu isti kao kad ljudi obavljaju te djelatnosti primjenom kreativnog ili teoretskog razmišljanja, pri čemu snose potpunu odgovornost za posljedice.

3. Umjetna inteligencija povećat će količinu predviđanja koja se mogu donositi u brojnim područjima, počevši od mjerljivih korelacija između podataka, koje su nevidljive ljudskom oku, ali su vidljive strojevima, čime olakšava naše živote i rješava brojne probleme, ali će istovremeno narušiti našu sposobnost tumačenja uzročno-posljedične veze između ishodâ, na način da će pojmovi transparentnosti, ljudskog nadzora i odgovornosti nad rezultatima biti uvelike ugroženi.

[1] SL L 295, 21.11.2018., str. 39. – 98.
[2] Upućivanja na „države članice” u ovom dokumentu treba tumačiti kao upućivanja na „države članice EGP-a”.

4. Podaci (osobni i neosobni) u umjetnoj inteligenciji u mnogim su slučajevima ključna premisa za donošenje samostalnih odluka, što će nedvojbeno utjecati na živote pojedinaca na različitim razinama. Zbog toga EDPB i EDPS već u ovoj fazi ustrajno tvrde da Prijedlog uredbe o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) („Prijedlog")[3] ima **važne implikacije za zaštitu podataka**.

5. Dodjeljivanjem zadaće donošenja odluka strojevima, na temelju podataka, stvorit će se rizici za prava i slobode pojedinaca; to će utjecati na njihove privatne živote i može ugroziti određene skupine, pa čak i društva u cjelini. EDPB i EDPS naglašavaju da su prava na privatnost i na zaštitu osobnih podataka, koja su protivna pretpostavci da strojevi samostalno donose odluke, a na kojoj se temelji načelo umjetne inteligencije, okosnica vrijednosti EU-a priznatih u Općoj deklaraciji o ljudskim pravima (članak 12.), Europskoj konvenciji o ljudskim pravima (članak 8.) i Povelji EU-a o ljudskim pravima (dalje u tekstu: Povelja) (članci 7. i 8.). Pomirenje mogućnosti za rast koje nude primjene umjetne inteligencije s činjenicom da ljudi imaju središnji i glavni položaj u odnosu na strojeve vrlo je ambiciozan, ali nužan cilj.

6. EDPB i EDPS pozdravljaju činjenicu da su u uredbu uključeni svi dionici lanca vrijednosti umjetne inteligencije, kao i to da su uvedeni posebni zahtjevi za pružatelje rješenja jer oni imaju važnu ulogu u proizvodima koji skoriste njihove sustave. Međutim, odgovornosti različitih strana – korisnika, pružatelja, uvoznika ili distributera sustava umjetne inteligencije – moraju biti jasno utvrđene i dodijeljene. Prilikom obrade osobnih podataka osobitu pozornost valja pridati usklađenosti tih uloga i odgovornosti s pojmovima voditelja i izvršitelja obrade podataka koji su predviđeni okvirom za zaštitu podataka jer obje norme nisu podudarne.

7. Prijedlogom se daje važna uloga ljudskom nadzoru (članak 14.), što EDPB i EDPS pozdravljaju. Međutim, kako je prethodno navedeno, zbog snažnog mogućeg učinka određenih sustava umjetne inteligencije na pojedince ili skupine pojedinaca, stvarna središnja uloga ljudi trebala bi imati prednost nad visokokvalificiranim ljudskim nadzorom i zakonitom obradom jer se takvi sustavi temelje na obradi osobnih podataka ili obrađuju osobne podatke kako bi ispunili svoje zadaće. Na taj bi se način osiguralo poštovanje prava na to da osoba nije predmet odluke koja se isključivo temelji na automatskoj obradi podataka.

8. Nadalje, s obzirom na podatkovno intenzivnu narav brojnih primjena umjetne inteligencije, Prijedlogom bi se trebalo promicati usvajanje pristupa tehničke i integrirane zaštite podataka na svakoj razini, čime se jamči učinkovita provedba načelâ zaštite podataka (kako je predviđeno člankom 25. Opće uredbe o zaštiti podataka i člankom 27. Europske uredbe o zaštiti podataka) s pomoću najnovijih tehnoloških dostignuća.

9. Konačno, EDPB i EDPS naglašavaju da donose ovo zajedničko mišljenje samo kao preliminarnu analizu Prijedloga, ne dovodeći u pitanje daljnju procjenu i mišljenja o učincima Prijedloga i njegovoj spojivosti sa zakonodavstvom EU-a u području zaštite podataka.

[3] COM(2021) 206 final.

2 ANALIZA KLJUČNIH NAČELA PRIJEDLOGA

2.1 Područje primjene Prijedloga i njegov odnos s postojećim pravnim okvirom

10. Kako je navedeno u obrazloženju, **pravna osnova** za Prijedlog prvenstveno je članak 114. UFEU-a, kojim se predviđa donošenje mjera za osiguravanje uspostave i funkcioniranja unutarnjeg tržišta[4]. Nadalje, Prijedlog se temelji i na članku 16. UFEU-a *jer sadržava određena posebna pravila o zaštiti pojedinaca u pogledu obrade osobnih podataka*, prije svega ograničenja uporabe sustava umjetne inteligencije za daljinsku biometrijsku identifikaciju ‚u stvarnom vremenu' na javnim mjestima za potrebe kaznenog progona[5].

11. EDPB i EDPS podsjećaju da, sukladno sudskoj praksi Suda, članak 16. UFEU-a predstavlja odgovarajuću pravnu osnovu kad je zaštita osobnih podataka jedan od glavnih ciljeva ili bitnih sastavnica pravila koje je donio zakonodavac Unije[6]. Primjena članka 16. UFEU-a podrazumijeva i potrebu za osiguranjem neovisnog nadzora za potrebe usklađenosti sa zahtjevima koji se odnose na obradu osobnih podataka, što je također propisano člankom 8. Povelje.

12. EDPS i EDPB podsjećaju da već postoji sveobuhvatni okvir za zaštitu podataka donesen na temelju članka 16. UFEU-a, koji se sastoji od Opće uredbe o zaštiti podataka (GDPR)[7], Uredbe o zaštiti podataka za institucije, urede, tijela i agencije Europske unije (Europska uredba o zaštiti podataka – EUDPR)[8] i Direktive o izvršavanju zakonodavstva (LED)[9]. Kako je navedeno u Prijedlogu, samo se dodatna ograničenja sadržana u Prijedlogu koja se odnose na obradu biometrijskih podataka mogu smatrati utemeljenima na članku 16. UFEU-a, a time i da imaju istu pravnu osnovu kao i Opća uredba o zaštiti podataka, Europska uredba o zaštiti podataka ili Direktiva o izvršavanju zakonodavstva. To ima važan utjecaj na općeniti odnos Prijedloga s Općom uredbom o zaštiti podataka, Europskom uredbom o zaštiti podataka i Direktivom o izvršavanju zakonodavstva, kako je navedeno u nastavku.

13. Što se tiče **područja primjene Prijedloga**, EDPB i EDPS snažno pozdravljaju činjenicu da Prijedlog obuhvaća uporabu sustavâ umjetne inteligencije u institucijama, tijelima ili agencijama EU-a. Budući da način na koji se ovi subjekti koriste sustavima umjetne inteligencije također može imati značajan učinak na temeljna prava pojedinaca, slično uporabi unutar država članica EU-a, neophodno je da se novi regulatorni okvir za umjetnu inteligenciju

[4] Obrazloženje, str. 5.
[5] Obrazloženje, str. 6. Vidjeti također uvodnu izjavu 2. Prijedloga.
[6] Mišljenje od 26. srpnja 2017., *PNR Canada*, Postupak donošenja mišljenja 1/15, ECLI:EU:C:2017:592, t. 96.
[7] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1. – 88.).
[8] Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39. – 98.).
[9] 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 sprječavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL L 119, 4.5.2016., str. 89. – 131.).

primjenjuje na države članice EU-a i na institucije, tijela, urede i agencije EU-a kako bi se zajamčio dosljedan pristup u čitavoj Uniji. S obzirom na činjenicu da institucije, tijela, uredi i agencije EU-a mogu djelovati kao pružatelji i korisnici sustavâ umjetne inteligencije, EDPS i EDPB smatraju da je u potpunosti prikladno obuhvatiti te subjekte područjem primjene Prijedloga na temelju članka 114. UFEU-a.

14. Međutim, EDPB i EDPS ozbiljno su zabrinuti zbog isključenja međunarodne suradnje u području izvršavanja zakonodavstva iz područja primjene utvrđenog u članku 2. stavku 4. Prijedloga. Tim se isključenjem stvara značajan rizik od zaobilaženja propisa (npr. u trećim zemljama ili međunarodnim organizacijama koje se koriste visokorizičnim aplikacijama na koje se oslanjaju javna tijela u EU-u).

15. Razvoj i uporaba sustavâ umjetne inteligencije u brojnim će slučajevima obuhvaćati obradu osobnih podataka. Osiguranje jasnoće odnosa između ovog Prijedloga i postojećeg zakonodavstva EU-a u području zaštite podataka od najveće je važnosti. Prijedlogom se ne dovode u pitanje Opća uredba o zaštiti podataka, Europska uredba o zaštiti podataka i Direktiva o izvršavanju zakonodavstva, koje se njime nadopunjuju. Iako je uvodnim izjavama Prijedloga pojašnjeno da bi uporaba sustavâ umjetne inteligencije i dalje trebala biti usklađena sa zakonodavstvom u području zaštite podataka, **EDPB i EDPS snažno preporučuju da se u članku 1. Prijedloga pojasni da se zakonodavstvo Unije u području zaštite osobnih podataka**, osobito Opća uredba o zaštiti podataka, Europska uredba o zaštiti podataka, Direktiva o e-privatnosti[10] i Direktiva o izvršavanju zakonodavstva, primjenjuju na svaku obradu osobnih podataka koja je obuhvaćena područjem primjene Prijedloga. Odgovarajućom uvodnom izjavom također bi trebalo pojasniti da se Prijedlogom ne nastoji utjecati na primjenu postojećih zakona EU-a kojima je uređena obrada osobnih podataka, uključujući zadaće i ovlasti neovisnih nadzornih tijela nadležnih za praćenje usklađenosti s tim instrumentima.

2.2 Pristup koji se temelji na riziku

16. EDPB i EDPS pozdravljaju **pristup temeljen na riziku**, na kojem je Prijedlog zasnovan. Prijedlog bi se primjenjivao na sve sustave umjetne inteligencije, uključujući one koji ne obuhvaćaju obradu osobnih podataka, ali ipak mogu imati učinak na interese ili temeljna prava i slobode.

17. EDPB i EDPS primjećuju da su u nekim odredbama u Prijedlogu izostavljeni rizici za skupine pojedinaca ili društvo u cjelini (npr. kolektivni učinci s osobitom važnošću, kao što su diskriminacija skupine ili izražavanje političkih mišljenja na javnim mjestima). EDPB i EDPS također preporučuju procjenu i ublažavanje rizika sustavâ umjetne inteligencije za društvo/skupine.

18. EDPB i EDPS smatraju da treba pojasniti pristup temeljen na riziku na kojem je Prijedlog zasnovan i da načelo „rizika za temeljna prava" treba biti **usklađeno s Općom uredbom o zaštiti podataka** jer se odnosi na aspekte povezane sa zaštitom osobnih podataka. Neovisno o

[10] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), kako je izmijenjena Direktivom 2006/24/EZ i Direktivom 2009/136/EZ.

tome je li riječ o krajnjim korisnicima, ispitanicima ili drugim osobama na koje se odnosi sustav umjetne inteligencije, izostanak bilo kakvog upućivanja na pojedinca zahvaćenog sustavom umjetne inteligencije u tekstu doima se kao propust u Prijedlogu. Obveze nametnute dionicima u pogledu zahvaćenih osoba trebale bi konkretnije proizlaziti iz zaštite pojedinca i njegovih prava. Stoga EDPB i EDPS pozivaju zakonodavce da se u Prijedlogu izričito pozabave pitanjem **prava i pravnih lijekova dostupnih pojedincima** koji podliježu sustavima umjetne inteligencije.

19. EDPB i EDPS skreću pozornost na izbor koji se odnosi na pružanje iscrpnog popisa **visokorizičnih sustava umjetne inteligencije.** Ovaj izbor može dovesti do stvaranja učinka pretjerane pojednostavnjenosti, sa slabim sposobnostima privlačenja visokorizičnih situacija, čime se podriva sveukupni pristup temeljen na riziku na kojem je Prijedlog zasnovan. Osim toga, ovaj popis visokorizičnih sustava umjetne inteligencije podrobno prikazan u prilozima II. i III. Prijedlogu ne sadrži neke vrste slučajeva primjene koje obuhvaćaju značajne rizike, kao što je uporaba umjetne inteligencije za utvrđivanje premije osiguranja ili za ocjenjivanje medicinskih tretmana ili za svrhe zdravstvenog istraživanja. EDPB i EDPS također ističu da će biti potrebno redovno ažurirati te priloge kako bi se zajamčilo da je njihovo područje primjene prikladno.

20. Prijedlogom se od **pružatelja** sustava umjetne inteligencije zahtijeva da provode procjenu rizika; međutim, u većini slučajeva voditelji obrade (podataka) bit će **korisnici**, a ne pružatelji sustavâ umjetne inteligencije (npr. korisnik sustava prepoznavanja lica je ‚voditelj obrade', što znači da se na njega ne primjenjuju zahtjevi za pružatelje visokorizične umjetne inteligencije u skladu s Prijedlogom).

21. Nadalje, **ponekad neće biti moguće da pružatelj provede procjenu svih primjena** za sustav umjetne inteligencije. Prema tome, početna procjena rizika bit će općenitije naravi nego ona koju će provoditi korisnik sustava umjetne inteligencije. Čak i ako u početnoj procjeni rizika koju provodi pružatelj nije navedeno da je sustav umjetne inteligencije „visokorizičan" u skladu s Prijedlogom, time ne bi trebala biti isključena **naknadna (detaljnija) procjena** (procjena učinka na zaštitu podataka) u skladu s člankom 35. Opće uredbe o zaštiti podataka, člankom 39. Europske uredbe o zaštiti podataka ili u skladu s člankom 27. Direktive o izvršavanju zakonodavstva) **koju bi trebao provoditi korisnik sustava**, s obzirom na kontekst uporabe i specifične slučajeve primjene. Tumačenje pitanja hoće li u skladu s Općom uredbom o zaštiti podataka, Europskom uredbom o zaštiti podataka i Direktivom o izvršavanju zakonodavstva određena vrsta obrade vjerojatno dovesti do visokog rizika provodi se neovisno o Prijedlogu. Međutim, klasifikacija sustava umjetne inteligencije kao sustava koji predstavlja „visoki rizik" zbog svojeg učinka na temeljna prava[11] **dovodi do pretpostavke o „visokom**

[11] Agencija Europske unije za temeljna prava (FRA) već se bavila potrebom za provođenjem procjena učinka na temeljna prava prilikom uporabe umjetne inteligencije ili povezanih tehnologija. U svojem izvješću iz 2020. naslovljenom „Ispravno shvaćanje budućnosti – Umjetna inteligencija i temeljna prava" (*Getting the future right – Artificial intelligence and fundamental rights*), Agencija je utvrdila „opasnosti u uporabi umjetne inteligencije, primjerice u prognostičkom radu policije, postavljanju zdravstvenih dijagnoza, socijalnim uslugama i ciljanom oglašavanju" i istaknula je da bi „privatne i javne organizacije trebale provoditi procjene načina na koji umjetna inteligencija može ugroziti temeljna prava" u svrhu smanjenja negativnih učinaka na pojedince.

riziku" u skladu s Općom uredbom o zaštiti podataka, Europskom uredbom o zaštiti podataka i Direktivom o izvršavanju zakonodavstva u pogledu obrade osobnih podataka.

22. **EDPB i EDPS slažu se s dijelom Prijedloga u kojem je utvrđeno da klasifikacija nekog sustava umjetne inteligencije kao visokorizičnog ne podrazumijeva nužno da je on sam po sebi zakonit i da se korisnik njime može koristiti kao takvim. Voditelj obrade možda će morati ispuniti dodatne zahtjeve koji proizlaze iz zakonodavstva EU-a u području zaštite podataka.** Nadalje, razmišljanje na kojem se temelji članak 5. Prijedloga, prema kojem bi, za razliku od zabranjenih sustava, visokorizični sustavi mogli biti načelno dopustivi, u Prijedlogu treba spomenuti i odbaciti, osobito zbog toga što predložena oznaka CE ne podrazumijeva da je povezana obrada osobnih podataka zakonita.

23. Međutim, usklađenost s pravnim obvezama koje proizlaze iz zakonodavstva Unije (uključujući u području zaštite osobnih podataka) treba biti preduvjet za uvrštenje proizvoda na europsko tržište kao proizvoda s oznakom CE. U tu svrhu EDPB i EDPS **predlažu da se u poglavlje 2. glave III. Prijedloga uvrsti zahtjev za osiguranje usklađenosti s Općom uredbom o zaštiti podataka i Europskom uredbom o zaštiti podataka**. Revizija (koju provodi treća strana) tih zahtjeva mora se provesti prije označivanja oznakom CE u skladu s načelom odgovornosti. U kontekstu procjene koju provodi treća strana, osobito će biti bitna početna procjena učinka koju provodi pružatelj.

24. S obzirom na složenosti koje nastaju razvojem sustavâ umjetne inteligencije, valja istaknuti da bi tehničke značajke sustava umjetne inteligencije (npr. vrsta pristupa umjetnoj inteligenciji) mogle prouzročiti veće rizike. Stoga bi pri svakoj procjeni rizika sustava umjetne inteligencije trebalo razmotriti **tehničke značajke** zajedno s **konkretnim slučajevima primjene i kontekstom** u kojem se sustav upotrebljava.

25. S obzirom na prethodno navedeno, EDPB i EDPS preporučuju da se u Prijedlogu utvrdi da **pružatelj** mora provoditi početnu procjenu rizika predmetnog sustava umjetne inteligencije **uzimajući u obzir slučajeve primjene** (koji će biti utvrđeni u Prijedlogu, što će predstavljati, primjerice, dopunu Priloga III. točke 1. podtočke (a), u kojem nisu spomenuti slučajevi primjene biometrijskih sustava umjetne inteligencije te da **korisnik** sustava umjetne inteligencije, u svojstvu voditelja obrade podataka u skladu sa zakonodavstvom EU-a u području zaštite podataka (ako je to relevantno), provodi procjenu učinka na zaštitu podataka, kako je detaljno predviđeno člankom 35. Opće uredbe o zaštiti podataka, člankom 39. Europske uredbe o zaštiti podataka i člankom 27. Direktive o izvršavanju zakonodavstva, uzimajući u obzir ne samo tehničke značajke i **slučaj primjene**, nego i **specifični kontekst** u kojem će se umjetna inteligencija upotrebljavati.

26. Nadalje, potrebno je pojasniti neke izraze navedene u Prilogu III. Prijedlogu, primjerice izraz „osnovne privatne usluge" ili mali pružatelj koji koristi umjetnu inteligenciju za ocjenu kreditne sposobnosti za vlastitu uporabu.

2.3 Zabranjene primjene umjetne inteligencije

27. EDPB i EDPS smatraju da **intruzivne oblike umjetne inteligencije** – osobito one koji mogu utjecati na ljudsko dostojanstvo – valja smatrati zabranjenim sustavima umjetne inteligencije

u skladu s člankom 5. Prijedloga, a ne sustavima koji su samo razvrstani kao „visokorizični" u Prilogu III. Prijedlogu, kao što su oni pod br. 6. To se osobito primjenjuje na usporedbe podataka koje, kada se koriste u velikoj mjeri, također utječu na osobe koje nisu dale povoda za promatranje policije ili su dale vrlo malo povoda ili obradu kojom se ugrožava načelo ograničenja svrhe u skladu sa zakonodavstvom u području zaštite podataka. Primjena umjetne inteligencije u području djelovanja policije i provedbe zakona zahtijeva precizna, predvidljiva i proporcionalna pravila specifična za određeno područje kojima se trebaju biti uzeti u obzir interesi zahvaćenih osoba i učinci na funkcioniranje demokratskog društva.

28. Postoji rizik od toga da se članak 5. Prijedloga tek formalno bavi „vrijednostima" i zabranom sustava umjetne inteligencije koji su protivni takvim vrijednostima. Kriterijima iz članka 5. prema kojima se sustavi umjetne inteligencije „smatraju" zabranjenima **ograničeno je područje primjene zabrane** u toj mjeri da bi se u praksi moglo pokazati beznačajnim (npr. „uzrokuje ili bi mogao uzrokovati tjelesnu ili psihološku štetu" u članku 5. stavku 1. točkama (a) i (b); ograničenje za javne vlasti u članku 5. stavku 1. točki (c); nedorečeni tekst u točki (c) podtočkama i. i ii.; ograničenje na daljinsku biometrijsku identifikaciju u „stvarnom vremenu" bez jasne definicije itd.).

29. Primjena umjetne inteligencije za „društveno vrednovanje", kako je predviđeno člankom 5. stavkom 1. točkom (c) Prijedloga, može dovesti do diskriminacije i protivna je temeljnim vrijednostima EU-a. Prijedlogom su zabranjene samo prakse koje se provode ‚u određenom razdoblju' ili koje provode ‚tijela javne vlasti' ili koje se provode ‚u njihovo ime'. Privatna poduzeća, a osobito pružatelji usluga društvenih mreža ili pružatelji usluga u oblaku, mogu obrađivati goleme količine osobnih podataka i provoditi društveno vrednovanje. Zbog toga bi **Prijedlogom trebali biti zabranjeni svi oblici društvenog vrednovanja**. Valja primijetiti da su takve aktivnosti u kontekstu provedbe zakona već značajno ograničene člankom 4. Direktive o izvršavanju zakonodavstva, iako nisu zabranjene u praksi.

30. **Daljinska biometrijska identifikacija** pojedinaca na javnim mjestima predstavlja visoki rizik od zadiranja u privatni život pojedinaca. Stoga EDPB i EDPS **smatraju da je potreban stroži pristup**. Uporaba sustava umjetne inteligencije može predstavljati ozbiljne probleme u smislu proporcionalnosti jer može obuhvaćati obradu podataka neselektivnog i nerazmjernog broja ispitanika u svrhu identifikacije tek nekoliko pojedinaca (npr. putnici u zračnim lukama i na željezničkim kolodvorima). **Neometana** narav sustavâ za daljinsku biometrijsku identifikaciju također predstavlja probleme u pogledu transparentnosti i u vezi s pravnom osnovom za obradu u skladu s pravom EU-a (Direktiva o izvršavanju zakonodavstva, Opća uredba o zaštiti podataka, Europska uredba o zaštiti podataka i ostalo primjenjivo pravo). Još nije riješen problem koji se odnosi na način kako ispravno obavijestiti pojedince o toj obradi, kao i na učinkovito i pravodobno ostvarenje prava pojedinaca. Isto vrijedi za njegov **nepovratan, ozbiljan učinak na** (razumno) **očekivanje stanovništva da će biti anonimno na javnim mjestima**, što dovodi do izravnog negativnog učinka na slobodu izražavanja, okupljanja i udruživanja, kao i slobodu kretanja.

31. U članku 5. stavku 1. točki (d) Prijedloga naveden je opsežan **popis iznimnih slučajeva** u kojima je daljinska biometrijska identifikacija ‚u stvarnom vremenu' na javnim mjestima dopuštena za potrebe kaznenog progona. EDPB i EDPS **taj pristup smatraju manjkavim**

zbog nekoliko razloga: Prvo, nije jasno što se treba smatrati „znatnim kašnjenjem" i kako bi se ono trebalo smatrati olakotnom okolnošću uzimajući u obzir činjenicu da sustav za masovnu identifikaciju može identificirati na tisuće pojedinaca u samo nekoliko sati. Osim toga, intruzivnost obrade ne ovisi uvijek o tome provodi li se identifikacija u stvarnom vremenu ili ne. Naknadna daljinska biometrijska identifikacija u kontekstu političkih prosvjeda vjerojatno će imati značajan odvraćajući učinak na ostvarivanje temeljnih prava i sloboda, kao što su sloboda okupljanja i udruživanja te, općenito, na temeljna načela demokracije. Drugo, intruzivnost obrade ne ovisi nužno o njezinoj svrsi. Uporaba ovog sustava u druge svrhe, kao što je privatna sigurnost, predstavlja iste prijetnje za temeljna prava poštovanja privatnog i obiteljskog života i zaštite osobnih podataka. Konačno, čak i uz predviđena ograničenja, potencijalni broj osumnjičenika ili počinitelja kaznenih djela gotovo će uvijek biti „dovoljno velik" kako bi se opravdala stalna uporaba sustava umjetne inteligencije za otkrivanje osumnjičenika, unatoč dodatnim uvjetima utvrđenima u članku 5. stavcima 2. do 4. Prijedloga. Čini se da razmišljanjem na kojem se temelji Prijedlog nije uzeto u obzir da će, prilikom nadzora otvorenih područja, obveze koje proizlaze iz prava EU-a u području zaštite podataka morati biti ispunjene ne samo za osumnjičenike, nego i za sve koji se nadziru u praksi.

32. Zbog toga EDPB i EDPS **pozivaju na opću zabranu svih oblika primjene umjetne inteligencije za automatizirano prepoznavanje ljudskih obilježja na javnim mjestima, kao što su prepoznavanje lica, ali i načina kretanja, otisaka prstiju, DNK-a, glasa, načina tipkanja i drugih biometrijskih ili bihevioralnih signala, u svakom kontekstu.** U Prijedlogu se trenutačno slijedi pristup prema kojem su utvrđeni i pobrojani svi sustavi umjetne inteligencije koje valja zabraniti. Zbog toga bi, u svrhu dosljednosti, **sustave umjetne inteligencije za masovnu daljinsku identifikaciju na internetu** valjalo zabraniti u skladu s člankom 5. Prijedloga. Uzimajući u obzir Direktivu o izvršavanju zakonodavstva, Europsku uredbu o zaštiti podataka i Opću uredbu o zaštiti podataka, EDPS i EDPB ne mogu razlučiti kako bi ova vrsta prakse mogla ispunjavati zahtjeve u pogledu nužnosti i proporcionalnosti, a to u konačnici proizlazi iz onoga što Sud Europske unije i Europski sud za ljudska prava smatraju prihvatljivim smetnjama u smislu temeljnih prava.

33. Nadalje, EDPB i EDPS **predlažu** da se javnim tijelima i privatnim subjektima **zabrani korištenje sustava umjetne inteligencije kojima se pojedince na temelju biometrijskih identifikatora (npr. na temelju prepoznavanja lica) razvrstava u skupine na temelju etničke pripadnosti, roda, kao i političke ili seksualne orijentacije ili drugih osnova na temelju kojih je zabranjena diskriminacija u skladu s člankom 21. Povelje ili** sustava umjetne inteligencije koji nisu znanstveno potvrđeni ili koji su izravno protivni temeljnim vrijednostima EU-a (npr. poligraf, Prilog III. točka 6. podtočka (b) i točka 7. podtočka (a)). Isto tako, **u skladu s člankom 5. valja zabraniti „biometrijsku kategorizaciju"**.

34. **Na ljudsko dostojanstvo također utječe mogućnost da će računalo utvrditi ili klasificirati naše buduće ponašanje neovisno o našoj slobodnoj volji**. Sustavi umjetne inteligencije namijenjeni tijelima kaznenog progona za individualne procjene rizičnosti pojedinaca kako bi se procijenila rizičnost pojedinca za počinjenje ili ponovno počinjenje kaznenog djela, usp. Prilog III. točku 6. podtočku (a) ili za predviđanje počinjenja ili ponovnog počinjenja stvarnog ili mogućeg kaznenog djela na temelju izrade profila pojedinaca ili procjene osobina i

karakteristika ili prethodnog kriminalnog ponašanja, usp. Prilog III. točku 6. podtočku (e) koji se koriste u skladu s njihovom namjenom dovest će do ključnog podvrgavanja policije i donositelja odluka u pravosuđu, što će dovesti do objektivizacije zahvaćenog ljudskog bića. Takvi sustavi umjetne inteligencije koji zadiru u bit prava na ljudsko dostojanstvo trebali bi biti zabranjeni u skladu s člankom 5.

35. Nadalje, EDPB i EDPS smatraju da je primjena umjetne inteligencije za **izvođenje zaključaka o emocijama pojedinaca vrlo nepoželjna i da bi je valjalo zabraniti**, osim u određenim dobro definiranim slučajevima primjene, odnosno u svrhu pružanja zdravstvenih usluga ili istraživanja (npr. kod bolesnika kod kojih je prepoznavanje emocija važno), pri čemu uvijek moraju biti uspostavljene primjerene mjere zaštite te, naravno, podložno svim ostalim uvjetima zaštite podataka i ograničenjima, uključujući ograničenje svrhe.

2.4 Visokorizični sustavi umjetne inteligencije

2.4.1 Potreba za *ex ante* ocjenjivanjem sukladnosti koje provode vanjske treće strane

36. EDPB i EDPS pozdravljaju činjenicu da sustavi umjetne inteligencije koji predstavljaju visoki rizik moraju biti podvrgnuti prethodnom ocjenjivanju sukladnosti prije njihova stavljanja na tržište ili stavljanja u uporabu u EU-u. Ovaj je regulatorni model u načelu dobrodošao jer pruža dobru ravnotežu između poticanja inovativnosti i visokog stupnja proaktivne zaštite temeljnih prava. Kako bi se počeli koristiti u određenim okruženjima kao što su postupci donošenja odluka u institucijama koje pružaju javne usluge ili kritične infrastrukture, moraju biti utvrđeni načini na koje je moguće istražiti potpuni izvorni kod.

37. Međutim, EDPB i EDPS zalažu se za usvajanje postupka ocjenjivanja sukladnosti iz članka 43. Prijedloga u smislu da se za **visokorizičnu umjetnu inteligenciju općenito mora provesti *ex ante* ocjenjivanje sukladnosti koje provode treće strane**. Iako ocjenjivanje sukladnosti za visokorizičnu obradu osobnih podataka koje provode treće strane nije propisano Općom uredbom o zaštiti podataka ili Europskom uredbom o zaštiti podataka, rizici koje predstavljaju sustavi umjetne inteligencije još nisu u potpunosti jasni. Zbog toga bi se općenitim uključivanjem obveze ocjenjivanja sukladnosti koje provode treće strane dodatno ojačala pravna sigurnost i povjerenje u sve visokorizične sustave umjetne inteligencije.

2.4.2 Područje primjene uredbe također mora obuhvaćati sustave umjetne inteligencije koji se već koriste

38. U skladu s člankom 43. stavkom 4. Prijedloga, visokorizični sustavi umjetne inteligencije trebali bi biti podvrgnuti novom postupku ocjenjivanja sukladnosti kad god se bitno izmijene. Ispravno je zajamčiti da su sustavi umjetne inteligencije usklađeni sa zahtjevima Uredbe o umjetnoj inteligenciji tijekom njihova čitavog životnog ciklusa. Uredba se ne primjenjuje na sustave umjetne inteligencije koji su stavljeni na tržište ili u uporabu prije primjene predložene uredbe (ili 12 mjeseci nakon početka njezine primjene za opsežne informacijske sustave navedene u Prilogu IX.), ako ne dođe do ‚znatne promjene' u konceptu ili namjeni tih sustava (članak 83.).

39. Međutim, prag tih ‚znatnih promjena' nije jasan. Uvodnom izjavom 66. Prijedloga utvrđen je niži prag za provedbu novog postupka ocjenjivanja sukladnosti „kad god nastupi promjena koja bi mogla utjecati na usklađenost sustava". Sličan prag bio bi primjeren za članak 83., barem u pogledu visokorizičnih sustava umjetne inteligencije. Nadalje, kako bi se uklonili mogući nedostaci u zaštiti, sustavi umjetne inteligencije koji su već uspostavljeni i u uporabi, nakon određene faze provedbe, također moraju biti usklađeni sa svim zahtjevima Uredbe o umjetnoj inteligenciji.

40. Na sigurnost sustavâ umjetne inteligencije utječu i brojne mogućnosti obrade osobnih podataka i vanjski rizici. Činjenica da su u članku 83. istaknute „znatne promjene u konceptu ili namjeni" ne obuhvaća upućivanje na promjene vanjskih rizika. Stoga bi u članak 83. Prijedloga trebalo uvrstiti upućivanje na promjene scenarija mogućih prijetnji, koje proizlaze iz vanjskih rizika, kao što su kibernapadi, neprijateljski napadi ili obrazložene pritužbe potrošača.

41. Nadalje, budući da je početak primjene predviđen 24 mjeseca nakon stupanja na snagu buduće Uredbe, EDPS i EDPB ne smatraju primjerenim još dulje izuzimanje sustava umjetne inteligencije koji su već stavljeni na tržište. Iako se Prijedlogom predviđa i to da zahtjevi Uredbe moraju biti uzeti u obzir prilikom evaluacije svakog opsežnog informacijskog sustava, kako je predviđeno pravnim aktima navedenima u Prilogu IX., EDPB i EDPS smatraju da bi zahtjevi koji se odnose na stavljanje u uporabu sustava umjetne inteligencije trebali biti primjenjivi od datuma početka primjene buduće Uredbe.

2.5 Upravljanje i Europski odbor za umjetnu inteligenciju

2.5.1 Upravljanje

42. EDPB i EDPS pozdravljaju činjenicu da je EDPS imenovan nadležnim tijelom i tijelom za nadzor tržišta koje će provoditi nadzor nad institucijama, agencijama i tijelima EU-a kada su obuhvaćeni područjem primjene ovog Prijedloga. EDPS je spreman obavljati svoju novu ulogu regulatora u području umjetne inteligencije za javnu upravu EU-a. Nadalje, uloga i zadaće EDPS-a nisu dovoljno detaljno utvrđene i trebalo bi ih dodatno pojasniti u Prijedlogu, osobito kad je riječ o njegovoj ulozi tijela za nadzor tržišta.

43. EDPB i EDPS potvrđuju dodjelu financijskih sredstava, koja je Prijedlogom predviđena za Odbor i EDPS-a, koji djeluje u svojstvu tijela koje provodi prijavljivanje. Međutim, kako bi EDPS obavljao nove dužnosti koje su predviđene za njega, neovisno o tome djeluje li u svojstvu tijela koje provodi prijavljivanje, potrebni su znatno veći financijski i ljudski resursi.

44. Prvo, zbog činjenice da EDPS u skladu s tekstom članka 63. stavka 6. „djeluje kao [...] tijelo za nadzor tržišta" za institucije, agencije i tijela Unije koji su obuhvaćeni područjem primjene Prijedloga, pri čemu nije pojašnjeno treba li se EDPS smatrati u potpunosti „tijelom za nadzor tržišta", kako je predviđeno Uredbom (EU) 2019/1020. To stvara pitanja u pogledu dužnosti i ovlasti EDPS-a u praksi. Drugo, pod uvjetom da je odgovor na prethodno pitanje potvrdan, nije jasno na koji način uloga EDPS-a, kako je predviđeno Europskom uredbom o zaštiti podataka, može obuhvaćati zadatak predviđen člankom 11. Uredbe (EU) 2019/1020, koji obuhvaća „djelotvoran nadzor tržišta nad proizvodima koji su stavljeni na raspolaganje na internetu" ili „fizičk[e] i laboratorijsk[e] provjer[e] na temelju odgovarajućih uzoraka". Postoji rizik od toga

da bi preuzimanjem novog skupa zadataka bez daljnjih pojašnjenja u Prijedlogu moglo biti ugroženo izvršavanje njegovih obveza koje ima kao nadzornik za zaštitu podataka.

45. Međutim, EDPB i EDPS ističu da se neke odredbe Prijedloga kojima su definirane zadaće i ovlasti različitih nadležnih tijela sukladno Uredbi o umjetnoj inteligenciji, njihovi odnosi, njihova narav i jamstvo njihove neovisnosti čine nejasnima u ovoj fazi. Iako je Uredbom 2019/1020 propisano da tijelo za nadzor tržišta mora biti neovisno, nacrtom Uredbe nije utvrđeno da tijela za nadzor tržišta moraju biti neovisna; štoviše, njome je utvrđeno da moraju izvješćivati Komisiju o određenim zadaćama koje obavljaju tijela za nadzor tržišta, koja mogu biti različite institucije. Budući da je u Prijedlogu također navedeno da će tijela za zaštitu podataka biti tijela za nadzor tržišta za sustave umjetne inteligencije koji se upotrebljavaju za kazneni progon (članak 63. stavak 5.), to također znači da će, možda putem svojeg nacionalnog nadležnog tijela, podlijegati obvezama izvješćivanja Komisije (članak 63. stavak 2.), što se čini nespojivim s njihovom neovisnošću.

46. Stoga EDPB i EDPS smatraju da je potrebno pojasniti te odredbe kako bi bile dosljedne s Uredbom 2019/1020, Europskom uredbom o zaštiti podataka i Općom uredbom o zaštiti podataka te da bi Prijedlogom trebalo biti jasno utvrđeno da nadzorna tijela u skladu s Uredbom o umjetnoj inteligenciji moraju biti potpuno neovisna u obavljanju svojih zadaća jer bi to predstavljalo temeljno jamstvo za pravilan nadzor i provedbu buduće uredbe.

47. EDPB i EDPS također podsjećaju da tijela za zaštitu podataka već provode Opću uredbu o zaštiti podataka, Europsku uredbu o zaštiti podataka i Direktivu o izvršavanju zakonodavstva u pogledu sustava umjetne inteligencije koji obuhvaćaju osobne podatke kako bi zajamčili zaštitu temeljnih prava, a osobito prava na zaštitu podataka. Stoga tijela za zaštitu podataka u određenoj mjeri već razumiju tehnologije umjetne inteligencije, podatke i obradu podataka, temeljna prava i imaju određenu stručnost u ocjenjivanju rizika koje nove tehnologije predstavljaju za temeljna prava, kako se Prijedlogom zahtijeva za nacionalna nadležna tijela. Nadalje, kada se sustavi umjetne inteligencije temelje na obradi osobnih podataka ili kada obrađuju osobne podatke, odredbe Prijedloga izravno su međusobno povezane s pravnim okvirom za zaštitu podataka, što će biti slučaj za većinu sustava umjetne inteligencije obuhvaćenih područjem primjene uredbe. Zbog toga će doći do međusobne povezanosti ovlasti nadzornih tijela na temelju Prijedloga i tijelâ za zaštitu podataka.

48. Stoga bi se imenovanjem tijela za zaštitu podataka nacionalnim nadzornim tijelima zajamčio usklađeniji regulatorni pristup i doprinijelo bi se dosljednom tumačenju odredbi o obradi podataka te bi se izbjegle proturječnosti u njihovoj provedbi među državama članicama. Jedinstvena kontaktna točka za sve aktivnosti obrade podataka obuhvaćene područjem primjene Prijedloga i ograničenje interakcija između dvaju različitih regulatornih tijela za obradu na koja se odnose Prijedlog i Opća uredba o zaštiti podataka također bi donijeli koristi za dionike lanca vrijednosti umjetne inteligencije. Zbog toga EDPB i EDPS smatraju da bi **tijela za zaštitu podataka trebala biti imenovana nacionalnim nadzornim tijelima u skladu s člankom 59. Prijedloga.**

49. U svakom slučaju, budući da Prijedlog sadrži posebna pravila o zaštiti pojedinaca u vezi s obradom osobnih podataka donesena na temelju članka 16. UFEU-a, usklađenost s tim

pravilima, a osobito ograničenja primjene sustavâ umjetne inteligencije za daljinsku biometrijsku identifikaciju ‚u stvarnom vremenu' na javnim mjestima za potrebe kaznenog progona **mora podlijegati nadzoru neovisnih tijela**.

50. Međutim, u Prijedlogu ne postoji odredba kojom bi se ovlast za osiguranje usklađenosti s tim pravilima izričito dodijelila nadzoru neovisnih tijela. Jedino upućivanje na nadležna nadzorna tijela za zaštitu podataka na temelju Opće uredbe o zaštiti podataka ili Direktive o izvršavanju zakonodavstva postoji u članku 63. stavku 5. Prijedloga, ali samo kao na tijela za „nadzor tržišta" te s nekim drugim nadležnim tijelima. EDPB i EDPS smatraju da time nije zajamčena usklađenost sa zahtjevom za neovisni nadzor utvrđenim u članku 16. stavku 2. UFEU-a i članku 8. Povelje.

2.5.2 Europski odbor za umjetnu inteligenciju

51. Prijedlogom se uspostavlja „Europski odbor za umjetnu inteligenciju" (EAIB). EDPB i EDPS prepoznaju potrebu za dosljednom i usklađenom primjenom predloženog okvira, kao i za sudjelovanjem neovisnih stručnjaka u razvoju politike EU-a u području umjetne inteligencije. Prijedlogom je istodobno glavna uloga dodijeljena Komisiji. Komisija ne samo da bi bila dio EAIB-a, nego bi njime i predsjedala i imala bi pravo veta na donošenje poslovnika EAIB-a. To je protivno potrebi da europsko tijelo za umjetnu inteligenciju bude neovisno o bilo kakvom političkom utjecaju. Stoga EDPB i EDPS smatraju da bi se budućom Uredbom o umjetnoj inteligenciji **EAIB-u trebao dati veći stupanj autonomije** kako bi zaista mogao zajamčiti dosljednu primjenu uredbe na jedinstvenom tržištu.

52. EDPB i EDPS također primjećuju da EAIB nema ovlasti u vezi s provedbom predložene uredbe. Međutim, s obzirom na širenje sustavâ umjetne inteligencije na cijelom području jedinstvenog tržišta i vjerojatnost prekograničnih slučajeva, postoji potreba od ključne važnosti za usklađenom provedbom i pravilnom dodjelom ovlasti između nacionalnih nadzornih tijela. EDPB i EDPS stoga preporučuju da se u budućoj Uredbi o umjetnoj inteligenciji utvrde mehanizmi suradnje među nacionalnim nadzornim tijelima. EDPB i EDPS predlažu uvođenje mehanizma kojim se jamči jedinstvena kontaktna točka za pojedince na koje se zakonodavstvo odnosi, kao i za poduzeća, za svaki sustav umjetne inteligencije te da za sve organizacije koje djeluju u više od polovice država članica EU-a Europski odbor za umjetnu inteligenciju ima mogućnost imenovanja nacionalnog tijela koje će biti odgovorno za provedbu Uredbe o umjetnoj inteligenciji za taj sustav umjetne inteligencije.

53. Nadalje, s obzirom na neovisan položaj tijela koja će biti zastupljena u Odboru, potonji bi trebao imati pravo samoinicijativno djelovati, a ne samo pružati savjete i pomoć Komisiji. EDPB i EDPS stoga ističu potrebu za proširenjem misije dodijeljene Odboru, koja, osim toga, ne odgovara zadaćama utvrđenima Prijedlogom.

54. Kako bi ti zahtjevi bili ispunjeni, **EAIB mora imati dostatne i odgovarajuće ovlasti**, a njegov pravni status treba biti pojašnjen. Kako bi bitno područje primjene buduće uredbe ostalo relevantno, čini se da je u njezinu izradu potrebno uključiti tijela nadležna za njezinu provedbu. Stoga EDPB i EDPS preporučuju da se EAIB-u dodijeli ovlast za podnošenje prijedloga Komisiji o izmjenama Priloga I., kojim su definirane tehnike i pristup umjetne inteligencije, i

Priloga III., u kojem su navedeni visokorizični sustavi umjetne inteligencije iz članka 6. stavka 2. Prije svake izmjene tih priloga Komisija bi se također trebala savjetovati s EAIB-om.

55. Člankom 57. stavkom 4. Prijedloga predviđena je razmjena informacija između Odbora i drugih tijela, ureda, agencija i savjetodavnih skupina Unije. Uzimajući u obzir njezin dosadašnji rad u području umjetne inteligencije i njezinu stručnost u području ljudskih prava, EDPB i EDPS preporučuju razmatranje Agencije za temeljna prava kao jednog od promatrača pri Odboru.

3 INTERAKCIJA S OKVIROM ZA ZAŠTITU PODATAKA

3.1 Odnos Prijedloga i postojećeg prava EU-a u području zaštite podataka

56. Jasno definirani odnos između Prijedloga i postojećeg zakonodavstva u području zaštite prava neophodan je preduvjet za osiguranje poštovanja i primjene pravne stečevine EU-a u području zaštite osobnih podataka. To područje zakonodavstva EU-a, a osobito Opća uredba o zaštiti podataka, Europska uredba o zaštiti podataka i Direktiva o izvršavanju zakonodavstva, mora se smatrati preduvjetom na kojem se mogu temeljiti daljnji zakonodavni prijedlozi bez ugrožavanja postojećih odredbi, uključujući kad je riječ o ovlastima nadzornih tijela i upravljanju.

57. Stoga je, prema mišljenju EDPB-a i EDPS-a, važno da se u Prijedlogu jasno izbjegnu sve nedosljednosti i mogući sukobi s Općom uredbom o zaštiti podataka, Europskom uredbom o zaštiti podataka i Direktivom o izvršavanju zakonodavstva. Svrha navedenoga nije samo postizanje pravne sigurnosti, nego i izbjegavanje opasnosti od toga da Prijedlog ima posljedicu izravnog ili neizravnog ugrožavanja temeljnog prava na zaštitu osobnih podataka, kako je utvrđen člankom 16. UFEU-a i člankom 8. Povelje.

58. Strojevi za samostalno učenje mogu štititi osobne podatke pojedinaca samo ako je ta značajka ugrađena u njihov dizajn. Trenutačna mogućnost ostvarivanja pravâ pojedinaca u skladu s člankom 22. (Automatizirano pojedinačno donošenje odluka, uključujući izradu profila) Opće uredbe o zaštiti podataka ili člankom 23. Europske uredbe o zaštiti podataka, neovisno o svrhama obrade, također je od ključne važnosti. U tom pogledu, ostala prava ispitanikâ povezana s pravom na brisanje i pravom na ispravak u skladu sa zakonodavstvom u području zaštite podataka moraju biti predviđena sustavima umjetne inteligencije od samog početka, neovisno o odabranom pristupu umjetnoj inteligenciji ili tehničkoj arhitekturi.

59. Uporaba osobnih podataka za učenje sustavâ umjetne inteligencije može dovesti do stvaranja pristranih obrazaca donošenja odluka u srži sustava umjetne inteligencije. Stoga je potrebno zahtijevati različite mjere zaštite, a osobito kvalificirani ljudski nadzor u takvim postupcima, kako bi se zajamčilo poštovanje i osiguranje pravâ ispitanika te kako bi se izbjegli svi negativni učinci za pojedince. Nadležna tijela također bi trebala moći predlagati smjernice za ocjenjivanje pristranosti u sustavima umjetne inteligencije i pomagati u provedbi ljudskog nadzora.

60. Ispitanici uvijek trebaju biti obaviješteni o tome da se njihovi podaci koriste kako bi se sustavima umjetne inteligencije omogućilo učenje i/ili predviđanje, o pravnoj osnovi za takvu obradu te trebaju dobiti opće objašnjenje logike (postupka) i informacije o opsegu sustava umjetne inteligencije. U tom pogledu u tim slučajevima uvijek treba biti zajamčeno pravo pojedinaca na ograničenje obrade (članak 18. Opće uredbe o zaštiti podataka i članak 20. Europske uredbe o zaštiti podataka), kao i na brisanje podataka (članak 16. Opće uredbe o zaštiti podataka i članak 19. Europske uredbe o zaštiti podataka). Nadalje, voditelj obrade trebao bi imati izričitu obvezu da obavijesti ispitanika o primjenjivim rokovima za prigovor, ograničenje, brisanje podataka itd. Sustav umjetne inteligencije mora moći ispunjavati sve zahtjeve u pogledu zaštite podataka putem primjerenih tehničkih i organizacijskih mjera. Dodatna transparentnost trebala bi se postići pravom na objašnjenje.

3.2 Izolirana okruženja i daljnja obrada (članci 53. i 54. Prijedloga)

61. Važno je promicati europsku inovativnost putem alata kao što je izolirano okruženje u skladu s postojećim pravnim i moralnim granicama. Izolirano okruženje pruža mogućnost uspostavljanja zaštitnih mjera potrebnih za jačanje povjerenja i oslanjanja na sustave umjetne inteligencije. Stručnjacima za umjetnu inteligenciju u složenim će okruženjima možda biti teško ispravno odvagnuti sve interese. Djelovanjem u regulatornom izoliranom okruženju moguće je brže steći uvid, čime se potiču inovacije, osobito za mala i srednja poduzeća.

62. U članku 53. stavku 3. Prijedloga navedeno je da izolirana okruženja ne utječu na nadzorne i korektivne ovlasti. Iako je ovo pojašnjenje korisno, postoji i potreba za izradom smjernica o tome kako postići dobru ravnotežu između djelovanja u svojstvu nadzornog tijela s jedne strane i davanja detaljnih smjernica putem izoliranog okruženja s druge strane.

63. U članku 53. stavku 6. navedeno je da se modaliteti i uvjeti funkcioniranja izoliranih okruženja utvrđuju provedbenim aktima. Važno je izraditi posebne smjernice kako bi se zajamčile dosljednost i potpora u uspostavljanju i radu izoliranih okruženja. Međutim, mogućnost svake države članice da izolirano okruženje prilagodi svojim potrebama i lokalnim praksama može biti ograničena obvezujućim provedbenim aktima. Stoga EDPB i EDPS preporučuju da umjesto toga smjernice za izolirana okruženja daje Europski odbor za umjetnu inteligenciju.

64. Člankom 54. Prijedloga želi se utvrditi pravna osnova za daljnju obradu osobnih podataka za razvoj određenih sustava umjetne inteligencije u javnom interesu u regulatornom izoliranom okruženju za umjetnu inteligenciju. Odnos između članka 54. stavka 1. Prijedloga i članka 54. stavka 2., odnosno uvodne izjave 41. Prijedloga, a time i postojećeg prava EU-a u području zaštite podataka, i dalje je nejasan. Međutim, temelj za ‚daljnju obradu' već je uspostavljen Općom uredbom o zaštiti podataka i Europskom uredbom o zaštiti podataka. Postizanje ravnoteže između interesâ voditelja obrade i interesâ ispitanika ne mora ugroziti inovacije, osobito u pogledu slučajeva kada je dopuštanje daljnje obrade u interesu javnosti. Člankom 54. Prijedloga trenutačno nisu riješena dva važna problema: i. u kojim okolnostima i primjenom kojih (dodatnih) kriterija se odvaguju interesi ispitanikâ i ii. hoće li se ti sustavi umjetne inteligencije koristiti samo u izoliranom okruženju. EDPB i EDPS pozdravljaju zahtjev za pravom Unije ili države članice prilikom obrade osobnih podataka prikupljenih u skladu s

Direktivom o izvršavanju zakonodavstva u izoliranom okruženju, ali preporučuju da se dodatno utvrdi što se time podrazumijeva, na način koji je usklađen s Općom uredbom o zaštiti podataka i Europskom uredbom o zaštiti podataka, prvenstveno na način da se pojasni da bi pravna osnova takvih izoliranih okruženja trebala biti usklađena sa zahtjevima utvrđenima u članku 23. stavku 2. Opće uredbe o zaštiti podataka i članku 25. Europske uredbe o zaštiti podataka te da se utvrdi da svaka uporaba izoliranog okruženja mora biti podvrgnuta evaluaciji. To se odnosi i na potpuni popis uvjeta iz članka 54. stavka 1. točaka (b) do (j).

65. Neka dodatna razmatranja u pogledu ponovne uporabe podataka iz članka 54. Prijedloga upućuju na to da je rad izoliranog okruženja intenzivan u smislu resursa, zbog čega je realno procijeniti da će samo mali broj poduzeća imati priliku sudjelovati. Sudjelovanje u izoliranom okruženju može donijeti konkurentsku prednost. Kako bi se omogućila ponovna uporaba podataka, bilo bi potrebno pomno razmotriti kako odabrati sudionike kako bi se zajamčilo da su obuhvaćeni područjem primjene i kako bi se izbjeglo nepošteno postupanje. EDPB i EDPS zabrinuti su zbog toga da omogućivanje ponovne uporabe podataka unutar okvira izoliranog okruženja odstupa od pristupa odgovornosti iz Opće uredbe o zaštiti podataka, pri čemu odgovornost snosi voditelj obrade, a ne nadležno tijelo.

66. Nadalje, EDPB i EDPS smatraju da, s obzirom na ciljeve izoliranog okruženja, a to su razvoj, testiranje i validacija sustava umjetne inteligencije, izolirana okruženja ne mogu biti obuhvaćena područjem primjene Direktive o izvršavanju zakonodavstva. Iako je Direktivom o izvršavanju zakonodavstva predviđena ponovna uporaba podataka za potrebe znanstvenog istraživanja, podaci obrađeni u sekundarne svrhe više neće podlijegati Direktivi o izvršavanju zakonodavstva, nego Općoj uredbi o zaštiti podataka ili Europskoj uredbi o zaštiti podataka.

67. Nije jasno što će sve regulatorno izolirano okruženje obuhvaćati. Postavlja se pitanje obuhvaća li predloženo regulatorno izolirano okruženje informacijsku infrastrukturu u svakoj državi članici s dodatnim pravnim osnovama za daljnju obradu ili je njime tek organiziran pristup regulatornoj stručnosti i smjernicama. EDPB i EDPS potiču zakonodavca da u Prijedlogu pojasni ovo načelo i da jasno navede kako regulatorno izolirano okruženje ne podrazumijeva obvezu nadležnih tijela da osiguraju njegovu tehničku infrastrukturu. U svakom slučaju nadležnim tijelima moraju biti pruženi financijski i ljudski resursi u skladu s takvim pojašnjenjem.

68. Konačno, EDPB i EDPS žele naglasiti razvoj prekograničnih sustava umjetne inteligencije, koji će biti dostupni na čitavom europskom digitalnom jedinstvenom tržištu. U slučaju takvih sustava umjetne inteligencije regulatorno izolirano okruženje kao alat za inovativnost ne bi trebalo postati prepreka za prekogranični razvoj. Stoga EDPB i EDPS preporučuju koordinirani prekogranični pristup koji je i dalje dovoljno dostupan na nacionalnoj razini svim MSP-ovima i koji pruža zajednički okvir na razini Europe, pri čemu nema pretjerano ograničavajući učinak. Potrebno je postići ravnotežu između europske koordinacije i nacionalnih postupaka kako bi se izbjegle proturječnosti u provedbi buduće Uredbe o umjetnoj inteligenciji, što bi predstavljalo prepreku za inovacije na razini čitavog EU-a.

3.3 Transparentnost

69. EDPB i EDPS pozdravljaju obvezu registriranja visokorizičnih sustava umjetne inteligencije u javnoj bazi podataka (kako je navedeno u člancima 51. i 60. Prijedloga). Ova baza podataka treba se smatrati prilikom za pružanje informacija široj javnosti o području primjene sustava umjetne inteligencije te o poznatim nedostacima i incidentima koji bi mogli ugroziti njihovo funkcioniranje, kao i o pravnim lijekovima koje su pružatelji donijeli kako bi ih riješili i uklonili.

70. Uporaba sustava provjere i ravnoteže ključno je demokratsko načelo. Stoga činjenica da se obveza transparentnosti ne primjenjuje na sustave umjetne inteligencije koji se koriste za otkrivanje, sprječavanje, istragu i kazneni progon kaznenih djela predstavlja preširoku iznimku. Valja razlikovati sustave umjetne inteligencije koji se koriste za otkrivanje ili sprječavanje od sustava umjetne inteligencije čija je svrha istraživanje ili pružanje pomoći u progonu kaznenih djela. Zaštitne mjere za sprječavanje i otkrivanje moraju biti jače zbog pretpostavke nedužnosti. Nadalje, EDPB i EDPS izražavaju žaljenje zbog nepostojanja upozorenja u Prijedlogu, što se može protumačiti kao zeleno svjetlo za uporabu čak i nedokazanih visokorizičnih sustava ili aplikacija umjetne inteligencije.

71. U slučajevima kada se javnosti može pružiti malo ili nimalo transparentnosti zbog tajnosti, čak i u funkcionalnoj demokraciji, moraju biti uspostavljene zaštitne mjere, a ti sustavi umjetne inteligencije trebaju biti registrirani i pružati transparentnost nadležnom nadzornom tijelu.

72. Osiguranje transparentnosti u sustavima umjetne inteligencije vrlo je izazovan cilj. U potpunosti kvantitativan pristup donošenju odluka u brojnim sustavima umjetne inteligencije, što se inherentno razlikuje od ljudskog pristupa, koji se uvelike oslanja na uzročno-posljedične veze i teoretsko razmišljanje, može biti protivan potrebi za prethodnim razumljivim objašnjenjem strojnog ishoda. Uredbom bi se trebali promicati novi, proaktivniji i pravodobni načini obavještavanja korisnika sustava umjetne inteligencije o statusu (donošenja odluka) sustava u bilo kojem trenutku, i to pružanjem ranog upozorenja o mogućim štetnim ishodima, kako bi pojedinci čija bi prava i slobode mogli biti ugroženi autonomnim odlukama stroja mogli reagirati na odluku ili potražiti pravnu zaštitu.

3.4 Obrada posebnih kategorija podataka i podaci povezani s kaznenim djelima

73. Obrada posebnih kategorija podataka u području izvršavanja zakonodavstva uređena je odredbama okvira EU-a za zaštitu podataka, uključujući Direktivu o izvršavanju zakonodavstva, kao i njezinu nacionalnu provedbu. U Prijedlogu se tvrdi da on ne pruža opću pravnu osnovu za obradu osobnih podataka, uključujući posebne kategorije osobnih podataka; usp. uvodnu izjavu 41. Međutim, članak 10. stavak 5. Prijedloga glasi: „Dobavljači visokorizičnih UI sustava mogu [...] obrađivati posebne kategorije osobnih podataka”. Nadalje, istom odredbom zahtijevaju se dodatne zaštitne mjere i navode se primjeri. Prema tome, čini se da je Prijedlog protivan primjeni Opće uredbe o zaštiti podataka, Direktive o izvršavanju zakonodavstva i Europske uredbe o zaštiti podataka. Iako EDPB i EDPS pozdravljaju pokušaj utvrđivanja primjerenih zaštitnih mjera, potreban je dosljedniji regulatorni pristup jer se trenutačne odredbe ne čine dovoljno jasnima kako bi njima bila uspostavljena pravna osnova za obradu posebnih kategorija podataka te moraju biti dopunjene dodatnim mjerama zaštite, koje trebaju biti ocijenjene.

Nadalje, kada su osobni podaci prikupljeni obradom sukladno području primjene Direktive o izvršavanju zakonodavstva, morat će se uzeti u obzir dodatne zaštitne mjere i ograničenja koji proizlaze iz nacionalnih propisa kojima se prenosi Direktiva o izvršavanju zakonodavstva.

3.5 Mehanizmi za postizanje usklađenosti

3.5.1 Certifikacija

74. Certifikacija je jedan od glavnih stupova Prijedloga. Sustav certifikacije prikazan u Prijedlogu temelji se na strukturi subjekata (tijela koja provode prijavljivanje / prijavljena tijela / Komisija) i mehanizmu za ocjenjivanje/certificiranje usklađenosti koji obuhvaća obavezne zahtjeve primjenjive na visokorizične sustave umjetne inteligencije te na europskim usklađenim normama u skladu s Uredbom (EU) br. 1025/2012 i zajedničkim specifikacijama koje će utvrditi Komisija. Mehanizam se razlikuje od sustava certifikacije usmjerenog na osiguranje usklađenosti s pravilima i načelima zaštite podataka, koji je određen u člancima 42. i 43. Opće uredbe o zaštiti podataka. Međutim, nije jasno kako se potvrde koje izdaju prijavljena tijela u skladu s Prijedlogom mogu povezivati s mehanizmima certificiranja, pečata i oznaka za zaštitu podataka predviđenima Općom uredbom o zaštiti podataka, za razliku od onog što je predviđeno za druge vrste potvrda (vidjeti članak 42. stavak 2. u pogledu potvrda koje se izdaju u skladu s Uredbom (EU) 2019/881).

75. Budući da se visokorizični sustavi umjetne inteligencije temelje na obradi osobnih podataka ili obrađuju osobne podatke kako bi izvršavali svoju zadaću, ove neusklađenosti mogu dovesti do pravnih nesigurnosti za sva dotična tijela jer mogu dovesti do situacija u kojima bi se sustavi umjetne inteligencije certificirani u skladu s Prijedlogom i označeni oznakom sukladnosti CE nakon stavljanja na tržište ili u uporabu mogli koristiti na način koji nije usklađen s pravilima i načelima zaštite podataka.

76. U Prijedlogu nedostaje izravna poveznica s pravom o zaštiti podataka i ostalim pravom EU-a i država članica primjenjivim na svako ‚područje' visokorizičnog sustava umjetne inteligencije navedenog u Prilogu III. S obzirom na činjenicu da visokorizični sustavi umjetne inteligencije uvelike zadiru u temeljna prava na privatnost i zaštitu osobnih podataka te potrebu za osiguranjem visoke razine povjerenja u sustav umjetne inteligencije, Prijedlog bi osobito trebao sadržavati načela smanjenja količine podataka i tehničke zaštite podataka kao jedan od aspekata koje valja razmotriti prije ishođenja oznake CE. Stoga EDPB i EDPS predlažu da se Prijedlog izmjeni na način da se pojasni odnos između potvrda izdanih u skladu s navedenom Uredbom i mehanizama certificiranja, pečata i oznaka za zaštitu podataka. Konačno, tijela za zaštitu podataka trebala bi sudjelovati u izradi i uspostavi usklađenih normi i zajedničkih specifikacija.

77. U vezi s člankom 43. Prijedloga, što se tiče ocjenjivanja sukladnosti, čini se da je odstupanje od postupka ocjenjivanja sukladnosti utvrđeno u članku 47. vrlo široko i obuhvaća previše iznimaka, kao što su iznimni razlozi javne sigurnosti ili zaštite života i zdravlja ljudi, zaštite okoliša i zaštite ključne industrijske i infrastrukturne imovine. Predlažemo zakonodavcima da smanje njihov broj.

3.5.2 Kodeksi ponašanja

78. Kako je navedeno u članku 69. Prijedloga, Komisija i države članice potiču i olakšavaju izradu kodeksa ponašanja kojima bi se pružatelje sustava umjetne inteligencije koji nisu visokorizični potaknulo da dobrovoljno primjenjuju zahtjeve koji su primjenjivi na visokorizične sustave umjetne inteligencije, kao i dodatne zahtjeve. U skladu s uvodnom izjavom 78. Opće uredbe o zaštiti podataka, EDPB i EDPS preporučuju utvrđivanje i definiranje sinergija između tih instrumenata i kodeksa ponašanja predviđenih Općom uredbom o zaštiti podataka kojima se pruža potpora usklađenosti u pogledu zaštite podataka. U tom je kontekstu relevantno pojasniti treba li se zaštita osobnih podataka smatrati jednim od „dodatnih zahtjeva" kojima se mogu baviti kodeksi ponašanja iz članka 69. stavka 2. Također je važno zajamčiti da su „tehničke specifikacije i rješenja" kojima se bave kodeksi ponašanja iz članka 69. stavka 1. osmišljeni na način da se njima potiče usklađenost sa zahtjevima nacrta uredbe o umjetnoj inteligenciji i da nisu protivni pravilima i načelima Opće uredbe o zaštiti podataka i Europske uredbe o zaštiti podataka. Time bi činjenica da se pružatelji sustava umjetne inteligencije koji nisu visokorizični, pod uvjetom da se takvi sustavi temelje na obradi osobnih podataka ili da obrađuju osobne podatke kako bi obavljali svoju zadaću, pridržavaju tih instrumenata predstavljala dodanu vrijednost jer će se time zajamčiti da će voditelji i izvršitelji obrade moći ispunjavati svoje obveze u pogledu zaštite podataka prilikom uporabe tih sustava.

79. Istodobno bi se uspostavio pravni okvir za pouzdanu umjetnu inteligenciju, dopunjen integracijom kodeksa ponašanja, u svrhu poticanja povjerenja u uporabu te tehnologije na način koji je siguran i usklađen sa zakonom, uključujući poštovanje temeljnih prava. Međutim, osmišljavanje tih instrumenata treba biti ojačano predviđanjem mehanizama usmjerenih na provjeru toga mogu li takvi kodeksi predstavljati učinkovite „tehničke specifikacije i rješenja" i mogu li se njima utvrditi „jasni ciljev[i] i ključni pokazatelj[i] uspješnosti za mjerenje ostvarenja tih ciljeva" kao sastavnih dijelova predmetnih kodeksa. Nadalje, nepostojanje upućivanja na (obavezne) mehanizme praćenja za kodekse ponašanja kojima bi se provjeravala usklađenost pružatelja sustava umjetne inteligencije koji nisu visokorizični s njihovim odredbama, kao i mogućnosti pojedinačnih pružatelja da izrade (i sami provode) navedene kodekse (vidjeti odjeljak 5.2.7. obrazloženja) moglo bi dodatno oslabiti učinkovitost i provedivost tih instrumenata.

80. Konačno, EDPB i EDPS traže pojašnjenje u pogledu vrsta inicijativa koje Komisija može razvijati, u skladu s uvodnom izjavom 81. Prijedloga, „za lakše smanjivanje tehničkih zapreka prekograničnoj razmjeni podataka u svrhu razvoja umjetne inteligencije".

4 ZAKLJUČAK

81. Iako EDPB i EDPS pozdravljaju Prijedlog Komisije i smatraju da je takva uredba nužna kako bi se zajamčila temeljna prava građana i rezidenata EU-a, smatraju da je, kako bi se osigurala njegova primjenjivost i učinkovitost, Prijedlog potrebno prilagoditi u pogledu nekoliko pitanja.

82. S obzirom na složenost Prijedloga i pitanja koja se njime žele riješiti, preostaje još mnogo posla dok Prijedlog ne bude takav da može dovesti do funkcionalnog pravnog okvira kojim se učinkovito dopunjuje Opća uredba o zaštiti podataka u smislu zaštite temeljnih ljudskih prava uz istodobno poticanje inovacija. EDPB i EDPS i dalje će biti dostupni za pružanje potpore na tom putu.

U Bruxellesu 18. lipnja 2021.

Za Europski odbor za zaštitu podataka	Za Europskog nadzornika za zaštitu podataka
Predsjednica	Nadzornik
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI