



Vijeće  
Europske unije

Bruxelles, 12. rujna 2022.  
(OR. en)

12302/22

LIMITE

JUR 579  
TELECOM 364  
COSI 217  
JAI 1155  
ENFOPOL 451

---

---

Međuinstitucijski predmet:  
2021/0106(COD)

---

---

## MIŠLJENJE PRAVNE SLUŽBE <sup>1</sup>

---

Od: Pravna služba

---

Predmet: Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji

- Primjerenost članaka 114. i 16. UFEU-a kao pravnih osnova u odnosu na odredbe primjenjive na tijela kaznenog progona i pravosudna tijela

---

### I. UVOD

1. Predloženom uredbom utvrđuju se usklađena pravila za stavljanje na tržište i stavljanje u uporabu sustava umjetne inteligencije („UI sustavi”) u Uniji („predložena uredba”)<sup>2</sup>.

---

<sup>1</sup> Ovaj dokument sadrži pravni savjet zaštićen na temelju članka 4. stavka 2. Uredbe (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30. svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije, koji Vijeće Europske unije javno ne objavljuje. Vijeće zadržava sva prava u odnosu na svako neovlašteno objavljivanje.

<sup>2</sup> Dok. 8115/21.

2. Na sastanku Radne skupine za telekomunikacije i informacijsko društvo 7. travnja 2022. Pravna služba Vijeća intervenirala je u vezi s pitanjem primjerenosti dviju pravnih osnova (članci 16. i 114. UFEU-a) za predloženu uredbu o sustavima umjetne inteligencije („UI sustavi”). U objašnjenjima je potvrđeno da su članci 16. i 114. UFEU-a odgovarajuće pravne osnove prijedloga, a da primjena članka 87. stavka 2. UFEU-a umjesto članka 114. UFEU-a nije prikladna. Na zahtjev Radne skupine, u ovom se mišljenju u pisanom obliku predstavlja i dodatno razmatra intervencija koju je na tom sastanku izložio predstavnik Pravne službe Vijeća.
3. UI sustavi definirani su u članku 3. stavku 1. predložene uredbe. Općenito, oni odgovaraju određenim vrstama softvera. Predložena uredba primjenjuje se i na dobavljače koji stavljaju UI sustave na tržište i na dobavljače koji stavljaju UI sustave u uporabu. Osim toga, predložena uredba primjenjuje se i na korisnike. Dobavljač može biti fizička osoba, pravna osoba ili tijelo javne vlasti koje razvija UI sustav ili ima razvijen UI sustav s ciljem njegova stavljanja na tržište ili stavljanja u uporabu pod vlastitim imenom ili žigom. Korisnik može biti svaka fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje upotrebljava UI sustav u okviru svoje nadležnosti.

4. Na temelju definicija iz članka 3., tijela kaznenog progona i pravosudna tijela mogla bi se smatrati dobavljačima i/ili korisnicima UI sustava. UI sustavi čija je namjena, kako ju je definirao dobavljač, kazneni progon ili pravosuđe, klasificirani su kao visokorizični u skladu s Prilogom III. Stoga podliježu temeljnim zahtjevima (upravljanje rizikom, testiranje, upravljanje podacima, tehnička dokumentacija, transparentnost, ljudski nadzor, točnost, otpornost i kibersigurnost) i obvezama (kao što su sustavi upravljanja kvalitetom, tehnička dokumentacija, ocjenjivanje sukladnosti, korektivne mjere, obveza obavješćivanja, obveze uvoznika i distributera) te normama i ocjenjivanju sukladnosti. Ta usklađena pravila inspirirana su pravilima koja se primjenjuju na sigurnost proizvoda u Direktivi 2006/42/EZ (strojevi)<sup>3</sup> i Uredbi 2017/745 (medicinski proizvodi)<sup>4</sup>.
5. Kad je riječ o UI sustavima koji uključuju upotrebu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona, oni pripadaju kategoriji zabranjenih UI sustava. Ta zabrana upotrebe UI sustava ipak podliježe iznimkama. Naime, države članice mogu, ali ne moraju, odobriti upotrebu takvih sustava. Ako se takvi sustavi odobre, na njih se primjenjuju detaljna ograničenja i zaštitne mjere kako bi se njihova upotreba ograničila na ono što je strogo nužno i kako bi se zaštitilo temeljno pravo na zaštitu osobnih podataka. Ta ograničenja i zaštitne mjere predviđeni su u predloženoj uredbi na temelju članka 16. Ugovora o funkcioniranju Europske unije („UFEU”) i moraju se dopuniti nacionalnim pravom. Članak 5. stavak 1. točka (d) i stavci 2., 3. i 4. predložene uredbe stoga su *lex specialis* u odnosu na Direktivu 2016/680 (Direktiva o zaštiti podataka u području izvršavanja zakonodavstva, „LED”), koja je donesena na temelju članka 16. stavka 2. UFEU-a.

---

<sup>3</sup> Direktiva 2006/42/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o strojevima i o izmjeni Direktive 95/16/EZ, SL L 157, 9.6.2006., str. 24–86.

<sup>4</sup> Uredba (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima, o izmjeni Direktive 2001/83/EZ, Uredbe (EZ) br. 178/2002 i Uredbe (EZ) br. 1223/2009 te o stavljanju izvan snage direktiva Vijeća 90/385/EEZ i 93/42/EEZ, SL L 117, 5.5.2017., str. 1–175.

U skladu s člankom 5. stavkom 1. točkom (d) ciljevi tih sustava ograničeni su na:

- i) ciljane potrage za konkretnim potencijalnim žrtvama kaznenih djela, uključujući nestalu djecu;
- ii) sprečavanje konkretne, znatne i neposredne prijetnje životu ili tjelesnoj sigurnosti pojedinaca ili terorističkog napada;
- iii) otkrivanje, lociranje, identifikaciju ili progon počinitelja kaznenog djela ili osumnjičenika za kazneno djelo iz članka 2. stavka 2. Odluke o europskom uhiđbenom nalogu<sup>5</sup> koje je u državi članici kažnjivo najvišom kaznom zatvora ili oduzimanjem slobode od najmanje tri godine, kako je utvrđeno pravom te države članice.

U skladu s člankom 5. stavkom 3., upotreba takvih tehnologija od strane tijela kaznenog progona mora podlijegati prethodnom odobrenju pravosudnog ili upravnog tijela. U propisno opravdanim hitnim situacijama, međutim, upotreba sustava može početi bez odobrenja i odobrenje se može zatražiti tek tijekom ili nakon upotrebe.

Na temelju članka 5. stavka 4. država članica može odlučiti odobriti upotrebu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona i utvrditi potrebna podrobna pravila o podnošenju zahtjeva za prethodna odobrenja te izdavanju i izvršavanju tih odobrenja, kao i o povezanim kaznenim djelima.

6. Pravne osnove predložene uredbe su članak 16. UFEU-a (zaštita osobnih podataka) i članak 114. UFEU-a (funkcioniranje unutarnjeg tržišta). Stoga se postavlja pitanje primjerenosti tih pravnih osnova u odnosu na usklađena pravila koja se primjenjuju na UI sustave koje pružaju ili se njima koriste tijela kaznenog progona i pravosudna tijela.

---

<sup>5</sup> Okvirna odluka Vijeća 2002/584/PUP od 13. lipnja 2002. o Europskom uhiđbenom nalogu i postupcima predaje između država članica, SL L 190, 18.7.2002., str. 1.

7. Ovo je mišljenje usmjereno prvo na primjerenost članka 114. UFEU-a kao pravne osnove, u posebnom kontekstu tijela kaznenog progona koja su navedena u nekoliko odredaba predložene uredbe, tj. u pogledu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima i visokorizičnih UI sustava iz točke 6. Priloga III. Stoga se ono bavi pitanjem bi li, umjesto članka 114. UFEU-a (odjeljak II.), primjerenija pravna osnova za obuhvaćanje pružanja i upotrebe UI sustava od strane tijela kaznenog progona bio članak 87. stavak 2. UFEU-a (policajska suradnja). Po analogiji, zaključak iz ove napomene može se primijeniti na pravosudna tijela iz Priloga III. o visokorizičnim UI sustavima.
8. U ovoj se napomeni razmatra i primjerenost članka 16. UFEU-a kao dodatne pravne osnove i primjena protokola 21. i 22. u kontekstu upotrebe sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima od strane tijela kaznenog progona (odjeljak III.).

## II. PRIMJERENOST ČLANKA 114. UFEU-A KAO PRAVNE OSNOVE

9. Prema ustaljenoj sudskoj praksi pravna osnova akta Unije ne ovisi o uvjerenju institucije o cilju koji se nastoji ostvariti, već se mora odrediti na temelju objektivnih kriterija podložnih sudskom preispitivanju, koji posebno uključuju cilj i sadržaj mjere. Ako se razmatranjem mjere ustanovi da ona ima dvostruku svrhu ili dvije sastavnice i ako se može utvrditi da je jedna od tih svrha ili sastavnica glavna ili prevladavajuća, a druga tek sporedna, ta se mjera mora temeljiti na jednoj pravnoj osnovi, odnosno onoj koja je potrebna za glavnu ili prevladavajuću svrhu ili sastavnicu. Samo iznimno, ako se utvrdi da akt istodobno ima više neodvojivo povezanih ciljeva, a da ni jedan od njih nije sekundaran ili neizravan u odnosu na drugi, takav akt može se temeljiti na više odgovarajućih pravnih osnova, osim ako se tim pravnim osnovama propisuju postupci koji su međusobno nekompatibilni. Treba također napomenuti i da je iz prve rečenice članka 114. stavka 1. UFEU-a jasno da se odredbe iz tog članka primjenjuju „[a]ko drukčije nije predviđeno Ugovorima”. U skladu s tim, upotreba članka 114. UFEU-a opravdana je samo ako ne postoji određenija odredba koja može biti pravna osnova za dotičnu mjeru<sup>6</sup>. Ako Ugovor sadrži određeniju odredbu koja može biti pravna osnova za dotičnu mjeru, ta se mjera mora temeljiti na toj odredbi<sup>7</sup>.

---

<sup>6</sup> Mišljenje Pravne službe Vijeća od 17. svibnja 2016., 9007/16, točka 6.

<sup>7</sup> Presuda od 29. travnja 2004., *Komisija protiv Vijeća*, C-338/01, EU:C:2004:253, točka 60.

## A. CILJ PREDLOŽENE UREDBE

10. Predloženom uredbom usklađuje se stavljanje na tržište, stavljanje u uporabu i upotreba posebne vrste softvera (UI sustavi). Činjenica da javna tijela i privatni operateri mogu biti dobavljači ili korisnici takvih UI sustava nije sama po sebi nespojiva s člankom 114. UFEU-a kao pravnom osnovom<sup>8</sup>.
11. Nadalje, činjenica da tijela kaznenog progona ili oni koji djeluju u njihovo ime mogu biti među dobavljačima ili korisnicima takvih UI sustava nije dovoljna da bi se opravdala primjena članka 87. UFEU-a kao pravne osnove. Kako bi se utvrdilo je li to potrebno moraju se analizirati cilj i sadržaj predložene uredbe.
12. Cilj je predložene uredbe općenito, među ostalim u pogledu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima i visokorizičnih UI sustava, osigurati dosljednu i visoku razinu zaštite u cijeloj Uniji i spriječiti da slobodno kretanje UI sustava i povezanih proizvoda i usluga na unutarnjem tržištu ometaju njihove razlike. Njome se utvrđuju jedinstvene obveze za operatere i jamči ujednačena zaštita prevladavajućih razloga od javnog interesa i prava osoba na cijelom unutarnjem tržištu (uvodna izjava 2.). Preciznije, predloženom uredbom utvrđuju se pravila kojima se uređuje stavljanje na tržište i stavljanje u uporabu određenih UI sustava, te tako osigurava neometano funkcioniranje unutarnjeg tržišta i omogućuje da načela slobodnog kretanja robe i usluga pogoduju tim sustavima (uvodna izjava 5.). Općenito, prijedlogom se nastoji uspostaviti pouzdana integrirana umjetna inteligencija, primjenjiva na svim razinama, s potpunim skupom pravila za razvoj, stavljanje na tržište i upotrebu proizvoda, usluga i sustava temeljenih na umjetnoj inteligenciji. S obzirom na to da se UI već nalazi u velikom broju usluga i proizvoda te da će tako biti i u budućnosti, prijedlog slijedi logiku unutarnjeg tržišta utvrđivanjem „okvira za sigurnost proizvoda” koji se temelji na skupu od četiri kategorije rizika. Njime se propisuju zahtjevi za ulazak na tržište i certifikaciju visokorizičnih UI sustava s pomoću obaveznog postupka označivanja oznakom CE.

---

<sup>8</sup> Vidjeti pravno mišljenje Pravne službe Vijeća (ST 11395/14 točke od 39. do 41.) i presedane kao što su Direktiva (EU) 2016/2102 te direktive 2014/24/EU, 2014/25/EU i 2014/23/EU.

13. Nijedan od navedenih ciljeva predložene uredbe ne odnosi se na osiguravanje ciljeva javne sigurnosti. Čak i ako se ciljevi javne sigurnosti trebaju neizravno ostvariti usklađivanjem stavljanja na tržište / stavljanja u uporabu / upotrebe UI sustava od strane tijela kaznenog progona, Sud<sup>9</sup> je, tumačeći članak 87. stavak 2. UFEU-a s obzirom na članak 67. UFEU-a, naveo da, kako bi se akt Unije, uzimajući u obzir njegovu svrhu i sadržaj, temeljio na tom članku, on mora biti izravno povezan s ciljevima iz članka 67. UFEU-a (u ovom slučaju to su suzbijanje kriminaliteta i policijska suradnja). To je isključeno u kontekstu predložene uredbe jer su jedina usklađena pravila o upotrebi takvih sustava od strane tijela kaznenog progona (1) pravila o sigurnosti proizvoda koja se ujednačeno primjenjuju na sve dobavljače i korisnike u pogledu stavljanja na tržište / stavljanja u uporabu ili upotrebe UI sustava ili (2) pravila o zaštiti osobnih podataka, za koje je kao pravna osnova dodan članak 16. UFEU-a (vidjeti dio III. u nastavku).
14. U drugom slučaju<sup>10</sup>, iako je cilj izmjene Direktive o vatrenom oružju bio osigurati višu razinu javne sigurnosti u odnosu na terorističke prijetnje i druge oblike kaznenih djela, Sud je presudio da je usklađivanje aspekata koji se odnose na sigurnost robe jedan od ključnih elemenata za dobro funkcioniranje unutarnjeg tržišta, s obzirom na to da u tom području postoje različiti propisi koji mogu stvoriti prepreke trgovini<sup>11</sup>.

---

<sup>9</sup> Presuda od 6. svibnja 2014., *Europska komisija protiv Europskog parlamenta i Vijeće Europske unije*, C43/12, ECLI:EU:C:2014:298.

<sup>10</sup> Presuda od 3. prosinca 2019., *Češka Republika protiv Europskog parlamenta*, C-482/17, EU:C:2019:1035.

<sup>11</sup> Ibid., točka 57.: „Budući da je posebnost vatrenog oružja, suprotno onomu što tvrdi Republika Poljska, u tome što ono nije opasno samo za osobe koje se njime koriste, nego i za širu javnost, kao što je to Sud već istaknuo u točki 54. presude od 23. siječnja 2018., *Buhagiar i dr.* (C- 267/16, EU:C:2018:26), razmatranja u vezi s javnom sigurnosti nužna su u kontekstu propisa o nabavi i posjedovanju te robe, kao što se na to podsjeća u petoj uvodnoj izjavi Direktive 91/477.” Vidjeti i presudu od 23. siječnja 2018., *Albert Buhagiar i dr. protiv Minister for Justice*, C-267/16, EU:C:2018:26, točka 54.: „U tom pogledu važno je napomenuti da se, s obzirom na opasnost za sigurnost osoba koju predstavlja vatreno oružje, njegovo slobodno kretanje moglo postići samo strogim propisivanjem uvjeta njegova prijenosa među državama članicama, među kojima se nalazi načelo prethodnog odobrenja država članica uključenih u prijenos takve robe.”

15. Ciljevi predložene uredbe, uključujući članak 5. stavak 1. točku (d) te članak 5. stavke 2., 3. i 4. o upotrebi sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona i odredbe koje se odnose na visokorizične UI sustave iz točke 6. Priloga III., nisu izravno povezani s ciljem javne sigurnosti. Naprotiv, prijedlog daje odgovore na glavna pitanja koja se odnose na način na koji sustavi umjetne inteligencije utječu na zdravlje, sigurnost i temeljna prava. Stoga su relevantne odredbe izravno povezane s ciljem osiguravanja jednakih uvjeta za stavljanje na tržište / stavljanje u uporabu ili upotrebu UI sustava na unutarnjem tržištu, uz istodobnu zaštitu zdravlja, sigurnosti i temeljnih prava korisnika.
16. S obzirom na prethodno navedeno, glavni je cilj predložene uredbe poboljšati funkcioniranje unutarnjeg tržišta u smislu članka 114. UFEU-a, a ciljevi iz članka 67. UFEU-a samo su neizravno i uzgredno povezani s tim glavnim ciljem.

## **B. SADRŽAJ PREDLOŽENE UREDBE**

17. Predložena uredba u osnovi sadržava pravila o tome što je potrebno za stavljanje određenog proizvoda (UI softvera) na tržište (ili za njegovo stavljanje u uporabu) kako bi se osiguralo da je siguran i da poštuje temeljna prava. Njome se utvrđuje potpun skup pravila za razvoj, stavljanje na tržište i upotrebu proizvoda, usluga i sustava temeljenih na umjetnoj inteligenciji. Predloženom uredbom ne obvezuje se tijela kaznenog progona na upotrebu nekog UI sustava koji je zakonito stavljen na tržište niti se njome izravno uređuje način na koji bi tijela kaznenog progona trebala upotrebljavati takav UI sustav. Umjesto toga, njome se jasno određuju situacije u kojima se njegova planirana upotreba smatra visokorizičnom samom činjenicom da će UI sustav upotrebljavati tijela kaznenog progona ili pravosudna tijela.

18. Osim toga, članak 29. predložene uredbe sadržava pravila o uvjetima za upotrebu visokorizičnih UI sustava, ali ta odredba nije specifična za određeni sektor, ima ograničeno područje primjene (uglavnom u pogledu uputa za upotrebu proizvoda) i neodvojivo je povezana s obvezama koje su na temelju predložene uredbe nametnute proizvođačima UI sustava. Osim toga, državama članicama daje se određeni manevarski prostor za donošenje dodatnih pravila o upotrebi takvih visokorizičnih UI sustava. Kad je riječ o sustavima za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima koji se upotrebljavaju za potrebe kaznenog progona (članak 5.), predloženom uredbom djelomično se uređuje upotreba takvih sustava iz perspektive zaštite podataka na temelju članka 16. UFEU-a (vidjeti dio III. u nastavku).
19. Nadalje, jedino države članice mogu odlučiti hoće li predvidjeti mogućnost potpunog ili djelomičnog odobrenja upotrebe takvih sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu. Posebni uvjeti za takvu upotrebu trebaju biti utvrđeni u nacionalnom pravu, ali moraju biti u skladu s općim kriterijima i zaštitnim mjerama utvrđenima u Uredbi: prethodno sudsko ili upravno odobrenje, podnošenje zahtjeva za prethodno odobrenje te izdavanje i izvršavanje tog odobrenja, kao i navođenje kaznenih djela u vezi s kojima se takvi sustavi mogu upotrebljavati.

20. UI sustavi posebna su vrsta softvera. Usklađena pravila koja se primjenjuju na stavljanje na tržište ili u uporabu / upotrebu UI sustava stoga su usklađena pravila koja se odnose na sigurnost proizvoda. Primjenjuju se na jednak način, bez razlikovanja između javnih i privatnih korisnika. U skladu s relevantnim uvodnim izjavama predložene uredbe trebalo bi stoga osigurati dosljednu i visoku razinu zaštite u cijeloj Uniji. Istodobno bi trebalo spriječiti razlike koje otežavaju slobodno kretanje UI sustava i povezanih proizvoda i usluga na unutarnjem tržištu. To bi se postiglo utvrđivanjem jedinstvenih obveza za operatere i jamčenjem ujednačene zaštite prevladavajućih razloga od javnog interesa i prava osoba na cijelom unutarnjem tržištu, na temelju članka 114. UFEU-a<sup>12</sup>.
21. Predložena uredba sadržava nekoliko upućivanja na kazneni progon, upravljanje nadzorom granica i pravosuđe u Prilogu III. o visokorizičnim UI sustavima (točke 6., 7. i 8.). Ona uključuju detaljan i iscrpan popis u skladu s člankom 6. stavkom 2. uz ostale visokorizične sustave u vezi s rizicima za sigurnost proizvoda iz članka 6. stavka 1. Naime, u skladu s člankom 6. stavkom 1., neki UI sustavi sami po sebi smatraju se visokorizičnima zbog njihove očekivane ozbiljnosti i visokih rizika za temeljna prava, zdravlje i sigurnost. Ostali sustavi koji se smatraju visokorizičnima i navedeni su u Prilogu III. uključuju obrazovanje, upravljanje kritičnom infrastrukturom, zapošljavanje, biometrijsku identifikaciju i kategorizaciju te pristup osnovnim javnim i privatnim uslugama.

---

<sup>12</sup> Stoga je potreban pravni okvir kojim se utvrđuju usklađena pravila o umjetnoj inteligenciji kako bi se poticali razvoj, upotreba i prihvaćanje umjetne inteligencije na unutarnjem tržištu kojima se istodobno ostvaruje visoka razina zaštite javnih interesa, kao što su zdravlje i sigurnost te zaštita temeljnih prava koja su priznata i zaštićena pravom Unije. Kako bi se postigao taj cilj, trebalo bi utvrditi pravila kojima se uređuje stavljanje na tržište i stavljanje u uporabu određenih UI sustava, te tako osigurati neometano funkcioniranje unutarnjeg tržišta i omogućiti da načela slobodnog kretanja robe i usluga pogoduju tim sustavima (vidjeti uvodne izjave 2. i 5. Prijedloga).

22. Međutim, takvim pravilima o visokorizičnim UI sustavima ne propisuje se trebaju li tijela kaznenog progona i pravosudna tijela (ili ona iz drugih utvrđenih područja) upotrebljavati te sustave. Predložena uredba samo će neizravno utjecati na stvarni razvoj UI sustava koje tijela kaznenog progona mogu upotrebljavati te na UI sustave koji se upotrebljavaju sada ili će se upotrebljavati u budućnosti. Stoga se ta pravila odnose na UI sustave koji su „namijenjeni za upotrebu” od strane tih tijela (vidjeti npr. članak 3. stavak 12., članak 8. stavak 2. i Prilog III.). Uvrštavanje određenog UI sustava na popis visokorizičnih ima kao posljedicu primjenu posebnog skupa pravila o upravljanju rizicima, upravljanju podacima i tehničkim specifikacijama. Korisnici takvih visokorizičnih UI sustava moraju poštovati upute za upotrebu, voditi evidenciju i provoditi procjene učinka na zaštitu podataka.
23. Nadalje, obveze korisnika koje nisu povezane s uputama za upotrebu mogu se utvrditi pravom Unije ili nacionalnim pravom i ne dovodeći u pitanje diskrecijsko pravo korisnika da organizira svoje resurse i aktivnosti za potrebe provedbe mjera ljudskog nadzora koje je naveo dobavljač (članak 29. stavak 2. predložene uredbe). Tim se pravilima predviđaju dodatne mjere zaštite temeljnih prava za visokorizične UI sustave.

24. S obzirom na prethodno navedeno, trebalo bi naglasiti da predložena uredba ne sadržava pravila kojima se nastoji omogućiti ili spriječiti da tijela kaznenog progona upotrebljavaju visokorizične UI sustave koji su stavljeni na tržište. U skladu s predloženim pravilima na UI sustav koji su razvila ili koji upotrebljavaju tijela kaznenog progona kao rezultat predviđene upotrebe primjenjivat će se posebna oznaka (visokorizično). Ta bi upotreba bila uređena nacionalnim pravom, a o njoj bi u određenoj mjeri odlučivala sama tijela kaznenog progona. Predloženom uredbom utvrđuju se minimalni uvjeti upotrebe u članku 29. (ograničeni na upute za upotrebu) za visokorizične UI sustave, uključujući one navedene u točkama 6., 7. i 8. Priloga III., koji će biti dopunjeni nacionalnim pravom. Stoga bi u skladu s praksom Suda trebalo razlikovati, s jedne strane, planirani cilj predložene uredbe, a to nije uređivanje upotrebe UI sustava od strane tijela kaznenog progona, i, s druge strane, učinke koje ona može neizravno proizvesti<sup>13</sup>, a koji nisu relevantni za analizu primjerenosti pravne osnove.
25. Točke 6., 7. i 8. (o kaznenom progonu, migracijama i pravosuđu) ne prevladavaju među visokorizičnim UI sustavima. Naime, na temelju predložene uredbe visokorizični UI sustav nije nužno onaj koji je naveden u Prilogu III. Većina visokorizičnih sustava zapravo su oni koji su generički navedeni u članku 6. stavku 1. točkama (a) i (b) predložene uredbe (u vezi sa sigurnošću proizvoda). Ostali visokorizični UI sustavi navedeni su u Prilogu III., koji sadržava točke 1. (biometrijska identifikacija), 2. (kritična infrastruktura), 3. (obrazovanje i strukovno osposobljavanje) i 4. (zapošljavanje, upravljanje radnicima i pristup samozapošljavanju) koje se odnose na područja koja nisu pravosuđe i unutarnji poslovi („PUP”). Svi korisnici takvih visokorizičnih UI sustava podliježu jedinstvenom režimu uspostavljenom ne s obzirom na njihov poseban status (npr. jesu li gospodarski subjekt ili javno tijelo), nego iz perspektive zaštite zdravlja, sigurnosti i temeljnih prava.

---

<sup>13</sup> Vidjeti presudu Suda od 21. lipnja 2018., *Republika Poljska protiv Europskog parlamenta, Vijeća Europske unije*, C-5/16, EU:C:2018:483, točke od 63. do 68. i presudu Suda od 22. lipnja 2022., *Leistritz AG protiv LH*, C-534/20, EU:C:2022:495, točka 28.

26. Predložena uredba stoga sadržava usklađena pravila o stavljanju na tržište, stavljanju u uporabu i upotrebi UI sustava bez obzira na to upotrebljavaju li ih privatni operateri ili javna tijela, uključujući, uzgredno<sup>14</sup>, tijela kaznenog progona i pravosudna tijela.
27. Osim upotrebe sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona, što podliježe posebnim pravilima o obradi osobnih podataka (vidjeti dio III. u nastavku), predložena uredba ne sadržava usklađena pravila o upotrebi visokorizičnih UI sustava. Kao što je objašnjeno u točkama 18. i 19., upućivanje na upotrebu visokorizičnih UI sustava u biti se odnosi na upute za upotrebu proizvoda (članak 29.) i povezano je s obvezama proizvođača. Kako je istaknuto u točki 22., odluka o tome mogu li tijela kaznenog progona ili pravosudna tijela upotrebljavati visokorizični UI sustav koji je zakonito stavljen na tržište u skladu s predloženom uredbom spada pod nacionalno pravo i donose je nacionalna tijela.
28. Stoga članak 87. stavak 2. UFEU-a, a posebno njegova točka (a), nije primjerena pravna osnova za predloženu uredbu. Pravilima iz Prijedloga niti se promiču niti ometaju prikupljanje, pohrana, obrada, analiza i razmjena relevantnih informacija. Jednostavno, ako takve aktivnosti obavljaju tijela kaznenog progona, trebat će poštovati niz nespecifičnih, usklađenih uvjeta kako bi se zaštitila prava korisnika. Slično tome, navedeni ciljevi predložene uredbe ne uključuju razvoj zajedničkih istražnih tehnika. Predloženi zahtjevi u pogledu upotrebe visokorizičnih UI sustava nisu specifični za područje pravosuđa i unutarnjih poslova te se ne odnose na policijsku suradnju *stricto sensu* kako je definirana u UFEU-u.

---

<sup>14</sup> Vidjeti mišljenje Suda o Istanbulskoj konvenciji, A-1/19, EU:C:2021:198, posebno točke 298. i 301.

29. S obzirom na odredbe članka 5. stavka 4. predložene uredbe, država članica i dalje može odlučiti odobriti upotrebu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona. Ako tako odluči, država članica dužna je utvrditi potrebna detaljna pravila za podnošenje zahtjeva za prethodno odobrenje te izdavanje i izvršavanje tog odobrenja, kao i povezana kaznena djela kod kojih je upotreba dopuštena za istragu ili kazneni progon<sup>15</sup>. Na temelju ishoda rasprava u Vijeću, ta predložena pravila ne bi rezultirala dodjelom novih ovlasti odgovarajućim nacionalnim tijelima. Umjesto toga, upotreba postojećih ili mogućih budućih mehanizama ograničena je kako bi se osigurala zaštita prava na privatnost i osobnih podataka.
30. S obzirom na navedeno, članak 114. UFEU-a jedina je primjerena pravna osnova za usklađena pravila o visokorizičnim UI sustavima, uključujući pravila koja upotrebljavaju tijela kaznenog progona i pravosudna tijela, a svaka pravna osnova iz područja PUP-a iz dijela trećeg glave V. UFEU-a, kao što je članak 87. UFEU-a u pogledu tih usklađenih pravila, nije ni opravdana ni primjerena.

---

<sup>15</sup> Valja napomenuti da članak 5. stavak 4. Prijedloga ima određena obilježja slična članku 15. stavku 1. Direktive 2002/58 o e-privatnosti. Konkretno, njime se predviđa mogućnost da države članice odstupe od određenih zabrana utvrđenih u pravu Unije. S obzirom na ustaljenu sudsku praksu, nacionalne odredbe kojima se namjerava odstupiti od te zabrane nužno će biti obuhvaćene područjem primjene prava Unije, što će pak dovesti do primjene Povelje na njih.

### **III. PRIMJERENOST ČLANKA 16. KAO DODATNE PRAVNE OSNOVE**

31. Predložena uredba uključuje članak 16. UFEU-a kao pravnu osnovu u pogledu obrade osobnih podataka u području kaznenog progona u uvodnim izjavama 25. i 26., u kojima se upućuje na članak 6.a Protokola 21. i članak 2.a Protokola 22 o obradi osobnih podataka u području suzbijanja kriminaliteta. Prema mišljenju Komisije, članak 16. UFEU-a trebao bi služiti isključivo kao pravna osnova za odredbe kojima se ograničava obrada biometrijskih osobnih podataka na komplementaran način u usporedbi s Direktivom 2016/680 („Direktiva LED”). Članak 5. stavak 1. točka (d) formulirana je kao načelna zabrana na koju se primjenjuje skup od tri iznimke. Konkretno, upotreba sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona zabranjena je, osim ako je to nužno potrebno za (a) ciljanu potragu za potencijalnim žrtvama kaznenih djela, (b) sprečavanje neposrednog terorističkog napada ili napada na tjelesni integritet / život osobe, (c) lociranje ili identifikaciju ili kazneni progon počinitelja ili osumnjičenika za teško kazneno djelo (s upućivanjem na europski uhiđbeni nalog). Dodatni zahtjevi iz članka 5. stavaka 2., 3. i 4. za tu specifičnu upotrebu UI sustava od strane tijela kaznenog progona osobito su procjena nužnosti i proporcionalnosti, prethodno odobrenje (osim u hitnim situacijama) i odluka pojedine države članice o tome hoće li ili ne na nacionalnoj razini odobriti tu specifičnu upotrebu UI alata u takvim situacijama.
32. Članak 5. predstavlja detaljnu odredbu kojom se uređuje specifična upotreba UI alata kojom se ne samo dopunjuje postojeći zakonodavni okvir Unije (Direktiva LED, koja se i sama temelji na članku 16. UFEU-a), nego i zahtijeva nacionalni provedbeni okvir.

33. U biti, unatoč tome što je formulirano kao zabrana, za posebno pravilo iz članka 5. moglo bi se reći da se njime utvrđuje strog i izniman okvir općeg praćenja pojedinaca „u stvarnom vremenu” na javnim mjestima koje provode UI instrumenti kako bih se identificiralo. Također, zabrana se ne odnosi samo na jednostavnu upotrebu kamera za snimanje, već se odnosi i na upotrebu alata umjetne inteligencije za automatsko prepoznavanje ljudskih obilježja na javnim mjestima (obilježja poput lica, ali i hoda, otisaka prstiju, DNK-a, glasa, načina tipkanja i drugih biometrijskih ili bihevioralnih signala). To također podrazumijeva prikupljanje i identifikaciju povezanih osoba usporednom analizom / provjerom podataka. Osim toga, pravilo se mora ocijeniti i s obzirom na činjenicu da se može dopustiti i identifikacija na javnim mjestima u stvarnom vremenu koju provode privatni korisnici (za događaje kao što su nogometne utakmice).
34. Čini se da dodatna pojašnjenja koja je iznijela Komisija upućuju na to da trenutačno nijedna država članica nije uredila to specifično pitanje ili ga je možda uredio vrlo mali broj država članica, kako bi se tijelima kaznenog progona omogućilo da upotrebljavaju UI alate za otkrivanje pojedinaca na javnim mjestima u stvarnom vremenu. Međutim, iako u praktičnom smislu nisu dostavljeni čvrsti dokazi kojima bi se dokazalo da će se postojeće prakse i alati morati promijeniti, čini se da je jasno da će buduće istražne tehnike, forenzičke metode i pravila o prikupljanju dokaza morati uključivati taj pristup zabrane/iznimki.
35. Što se tiče pravne osnove, čini se da se odredbama kojima se ograničava obrada biometrijskih osobnih podataka na komplementaran način (u usporedbi s Direktivom LED) nastoji zaštititi osobne podatke utvrđivanjem primjerenih zaštitnih mjera. Takav je cilj neraskidivo povezan s ciljem odredbi koje ulaze u područje primjene članka 114. UFEU-a, pri čemu nijedan nije sporedan i neizravan u odnosu na drugi. Cilj je predložene uredbe utvrditi opći okvir za UI sustave u skladu s pristupom koji se temelji na riziku. U tom kontekstu horizontalna regulacija UI sustavâ može uključivati stroge zaštitne mjere koje se primjenjuju na taj određeni UI sustav otkrivanja u stvarnom vremenu. Takav poseban UI sustav koji sadržava primjerene mjere za zaštitu osobnih podataka stoga je neraskidivo povezan s općim ciljem poboljšanja funkcioniranja unutarnjeg tržišta i nije sekundaran ili neizravan u odnosu na njega. Stoga bi se predložena uredba trebala temeljiti na dvojnoj osnovi u skladu s relevantnom sudskom praksom (vidjeti prethodni stavak 9.).

36. Međutim, ostaje pitanje koja bi se pravna osnova trebala upotrebljavati za uređivanje obrade osobnih podataka koje bi upotrebljavali sustavi iz članka 5. od stavka 1. točke (c) do stavka 4. predložene uredbe. Naime, članak 87. stavak 2. točka (a) UFEU-a predstavlja pravnu osnovu za mjere tijela kaznenog progona u vezi sa sprečavanjem, otkrivanjem i istragom kaznenih djela, koje se odnose na prikupljanje, pohranu, obradu, analizu i razmjenu odgovarajućih podataka.
37. Međutim, kao što je to nezavisni odvjetnik objasnio u mišljenju o PNR-u za Kanadu (A1/15), članak 16. UFEU-a, s jedne strane, i članak 87. stavak 2. točka (a) i članak 82. stavak 1. točka (d) UFEU-a, s druge strane, ne mogu imati hijerarhijski odnos vrste „lex generalis – lex specialis”<sup>16</sup>. Članak 16. stavak 2. UFEU-a jedina je odredba koja se primjenjuje na pravila koja se odnose na zaštitu pojedinaca u vezi s obradom osobnih podataka od strane tijela kaznenog progona država članica pri provođenju aktivnosti za suzbijanje kriminaliteta. Činjenica da se u članku 5. upućuje na popis teških kaznenih djela iz Okvirne odluke o europskom uhidbenom nalogu ne mijenja tu ocjenu: to upućivanje ne znači da se ta okvirna odluka primjenjuje sama po sebi<sup>17</sup>. To je samo zakonodavna tehnika za popisivanje teških kaznenih djela bez potrebe za izradom zasebnog priloga.
38. Činjenica je da pravilo iz članka 5. nije uspostavljeno kao sredstvo daljnjeg razgraničavanja uvjeta primjene tih mjera povezanih s PUP-om, nego kako bi se osiguralo da se u budućnosti kod svake upotrebe biometrijske identifikacije „u stvarnom vremenu” u UI sustavima na odgovarajući način odgovori na pitanja koja se odnose na temeljna prava, a prvenstveno na potrebu da se osigura prikupljanje i obrada biometrijskih podataka uz poštovanje prava na privatnost i osobnih podataka.

U tom pogledu cilj Uredbe nije utvrditi novi, obavezni postupak specifičan za PUP, već se ona oslanja na iskušana i provjerena postupovna sredstva kako bi se osiguralo poštovanje temeljnih prava.

---

<sup>16</sup> Vidjeti mišljenje nezavisnog odvjetnika P. Mengozzija od 8. rujna 2016., *Nacrt sporazuma između Kanade i Europske unije*, mišljenje 1/15, EU:C:2016:656, točke od 112. do 120.

<sup>17</sup> Za provedbu tog popisa teških kaznenih djela u državama članicama vidjeti presudu Suda od 21. lipnja 2022., *Liga za ljudska prava protiv Vijeća ministara*, C-817/19, EU:C:2022:65, točke od 150. do 152.

39. Ako je članak 16. UFEU-a primjerena dodatna pravna osnova, postavlja se pitanje o primjeni članka 6.a i 2.a protokola 21. i 22. Kako je objašnjeno u uvodnim izjavama 25. i 26. Prijedloga, to znači da ako tijela kaznenog progona u Irskoj ili Danskoj upotrebljavaju sustave za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za sprečavanje kriminala i ako Irska ili Danska nisu obvezane odgovarajućim pravilima o policijskoj suradnji ili pravosudnoj suradnji u kaznenim stvarima, te dvije države članice neće biti obvezane člankom 5. stavkom 1. točkom (d) te člankom 5. stavcima 2. i 3. predložene uredbe. To ne znači da članak 5. stavak 1. točka (d) i članak 5. stavci 2. i 3. sadržavaju pravila o policijskoj suradnji, kao što su pravila o razmjeni informacija među tijelima kaznenog progona. To jednostavno znači da se člankom 5. stavkom 1. točkom (d) i člankom 5. stavcima 2. i 3. predložene uredbe, slično Direktivi 2016/680 („LED”) koja je *lex generalis* i donesena na temelju članka 16. UFEU-a, uređuje obrada biometrijskih osobnih podataka u posebnom kontekstu sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za suzbijanje kriminaliteta i ništa više. Prijedlog Komisije u tom pogledu slijedi pristup koji je zakonodavac Unije zauzeo za Direktivu LED, čime se potvrđuje da primjena članka 87. stavka 2. UFEU-a u tom kontekstu stoga nije opravdana.
40. Dodavanje članka 16. UFEU-a članku 114. UFEU-a u ovom je slučaju opravdano činjenicom da su članak 5. stavak 1. točka (d) i članak 5. stavci 2. i 3. jedini odobreni slučajevi kojima se uređuje upotreba UI sustava koji zadire u pravo na zaštitu osobnih podataka, što predstavlja *lex specialis* u odnosu na opći okvir za zaštitu podataka. Takva *lex specialis* pravila o zaštiti podataka kojima se utječe na upotrebu tih osjetljivih UI sustava ne mogu se smatrati sekundarnima ili neizravnima u odnosu na pravnu osnovu koja se odnosi na unutarnje tržište. Stoga je dodavanje članka 16. UFEU-a kao pravne osnove dovoljno opravdano u predloženoj uredbi, a pozivanje na članak 87. stavak 2. točku (a) UFEU-a nije primjereno.

#### IV. ZAKLJUČAK

41. S obzirom na prethodno navedeno Pravna služba Vijeća sljedećeg je mišljenja:

- a) pozivanje na članke 16. i 114. UFEU-a kao pravne osnove predložene uredbe opravdano je i primjereno;
  - b) pozivanje na članak 87. stavak 2. UFEU-a ili bilo koju drugu pravnu osnovu iz područja PUP-a nije opravdano ni primjereno u odnosu na usklađena pravila koja se primjenjuju na UI sustave koje mogu pružati ili upotrebljavati tijela kaznenog progona ili pravosudna tijela.
-