



Svet
Evropske unije

Bruselj, 12. september 2022
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

Medinstitucionalna zadeva:
2021/0106(COD)

MNENJE PRAVNE SLUŽBE ¹

Pošiljatelj:	pravna služba
Zadeva:	Predlog uredbe Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci – Ustreznost členov 114 in 16 PDEU kot pravnih podlag v zvezi z določbami, ki se uporabljajo za organe za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter pravosodne organe

I. UVOD

1. Predlagana uredba določa harmonizirana pravila za dajanje na trg in v uporabo umetnointeligenčnih sistemov v Uniji (v nadaljnjem besedilu: predlagana uredba)².

¹ Ta dokument vsebuje pravne nasvete, zaščitene s členom 4(2) Uredbe (ES) št. 1049/2001 Evropskega parlamenta in Sveta z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije, ki jih Svet Evropske unije ni javno objavil. V primeru nepooblaščne objave si Svet pridržuje vse pravice.

² Dok. 8115/21.

2. Pravna služba Sveta je na seji Delovne skupine za telekomunikacije in informacijsko družbo 7. aprila 2022 predstavila stališče glede ustreznosti dveh pravnih podlag (člena 16 in 114 PDEU) za predlagano uredbo o umetnointeligenčnih sistemih. Na podlagi pojasnil je bilo potrjeno, da sta člena 16 in 114 PDEU pravilni pravni podlagi predloga in da uporaba člena 87(2) PDEU namesto člena 114 PDEU ni primerna. Na zahtevo delovne skupine je v tem mnenju pisno predstavljeno in dodatno pojasnjeno stališče predstavnika pravne službe Sveta z navedene seje.
3. Umetnointeligenčni sistemi so opredeljeni v členu 3, točka (1), predlagane uredbe. Na splošno ustrezajo nekaterim vrstam programske opreme. Predlagana uredba se uporablja tako za ponudnike, ki dajejo umetnointeligenčne sisteme na trg, kot tudi za ponudnike, ki dajejo umetnointeligenčne sisteme v uporabo. Poleg tega se predlagana uredba uporablja tudi za uporabnike. Ponudnik je lahko fizična ali pravna oseba, javni organ ali drugo telo, ki razvije umetnointeligenčni sistem ali ima umetnointeligenčni sistem, razvit za dajanje na trg ali v uporabo pod svojim imenom ali blagovno znamko. Uporabnik je lahko vsaka fizična ali pravna oseba, javni organ, agencija ali kateri koli drug organ, ki umetnointeligenčni sistem uporablja v svoji pristojnosti.

4. V skladu z opredelitvami iz člena 3 bi se lahko organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter pravosodni organi šteli za ponudnike in/ali uporabnike umetnointeligenčnega sistema. Umetnointeligenčni sistemi, katerih predvideni namen, kot ga opredeli ponudnik, je preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali upravljanje pravosodja, so v Prilogi III uvrščeni med sisteme velikega tveganja. Zato zanje kot take veljajo bistvene zahteve (obvladovanje tveganja, testiranje, upravljanje podatkov, tehnična dokumentacija, preglednost, človekov nadzor, točnost, robustnost in kibernetika varnost) in obveznosti (kot so sistemi upravljanja kakovosti, tehnična dokumentacija, ugotavljanje skladnosti, popravni ukrepi, dolžnost obveščanja, obveznosti uvoznikov in distributerjev) ter standardi in ugotavljanje skladnosti. Ta harmonizirana pravila temeljijo na pravilih, ki se uporabljajo za varnost proizvodov v Direktivi 2006/42/ES (stroji)³ in Uredbi (EU) 2017/745 (medicinski pripomočki)⁴.
5. Umetnointeligenčni sistemi, ki vključujejo uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, spadajo v kategorijo prepovedanih umetnointeligenčnih sistemov. Vendar za to prepoved uporabe umetnointeligenčnih sistemov veljajo izjeme. Države članice lahko namreč dovolijo uporabo takih sistemov ali pa ne. Če so dovoljeni, zanje veljajo podrobne omejitve in zaščitni ukrepi, da se njihova uporaba omeji na to, kar je nujno potrebno, in da se zaščiti temeljna pravica do varstva osebnih podatkov. Te omejitve in zaščitni ukrepi so določeni v predlagani uredbi na podlagi člena 16 Pogodbe o delovanju Evropske unije (PDEU) in jih je treba dopolniti z nacionalnim pravom. Člen 5(1)(d), (2), (3) in (4) predlagane uredbe je *lex specialis* glede na Direktivo 2016/680 (direktiva o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj), ki je bila sprejeta na podlagi člena 16(2) PDEU.

³ Direktiva 2006/42/ES Evropskega parlamenta in Sveta z dne 17. maja 2006 o strojih in spremembah Direktive 95/16/ES (UL L 157, 9.6.2006, str. 24–86).

⁴ Uredba (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, spremembi Direktive 2001/83/ES, Uredbe (ES) št. 178/2002 in Uredbe (ES) št. 1223/2009 ter razveljavitvi direktiv Sveta 90/385/EGS in 93/42/EGS (UL L 117, 5.5.2017, str. 1–175).

V skladu s členom 5(1)(d) so cilji navedenih sistemov omejeni na:

- i) usmerjeno iskanje določenih potencialnih žrtev kaznivih dejanj, vključno s pogrešanimi otroki;
- ii) preprečitev konkretne, znatne in neposredne nevarnosti za življenje ali fizično varnost fizičnih oseb ali preprečitev terorističnega napada;
- iii) odkrivanje, lokalizacijo, identifikacijo ali pregon storilca ali osumljenca kaznivega dejanja iz člena 2(2) sklepa o evropskem nalogu za prijetje⁵, ki se v zadevni državi članici kaznuje z zaporno kaznijo ali ukrepom, vezanim na odvzem prostosti najmanj treh let, kot je določeno z zakonodajo te države članice.

V skladu s členom 5(3) mora uporabo takšnih tehnologij s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj predhodno dovoliti pravosodni ali upravni organ. Vendar se lahko v ustrezno utemeljenih nujnih primerih sistem začne uporabljati brez dovoljenja, dovoljenje pa se lahko zahteva med uporabo ali po njej.

V skladu s členom 5(4) se lahko država članica odloči, da dovoli uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ter opredeli potrebna podrobna pravila za zahtevo, izdajo in izvajanje predhodnega dovoljenja ter s tem povezana kazniva dejanja.

6. Pravni podlagi predlagane uredbe sta člena 16 PDEU (varstvo osebnih podatkov) in 114 PDEU (delovanje notranjega trga). Zato se postavlja vprašanje ustreznosti navedenih pravnih podlag glede na harmonizirana pravila, ki se uporabljajo za umetnointeligenčne sisteme, ki jih zagotavljajo ali uporabljajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter pravosodni organi.

⁵ Okvirni sklep Sveta 2002/584/PNZ z dne 13. junija 2002 o evropskem nalogu za prijetje in postopkih predaje med državami članicami (UL L 190, 18.7.2002, str. 1).

7. To mnenje se najprej osredotoča na ustreznost člena 114 PDEU kot pravne podlage v posebnem okviru organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki so navedeni v več določbah predlagane uredbe, tj. v zvezi s sistemi za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih in umetnointeligenčnimi sistemi velikega tveganja iz točke 6 Priloge III. Obravnava torej vprašanje, ali bi bil člen 87(2) PDEU (policijsko sodelovanje) ustrežnejša pravna podlaga za zagotavljanje in uporabo umetnointeligenčnih sistemov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj namesto člena 114 PDEU (oddelek II). Po analogiji se lahko zaključek iz tega dopisa uporabi za pravosodne organe iz Priloge III, ki se nanaša na umetnointeligenčne sisteme velikega tveganja.
8. V tem dopisu sta obravnavani tudi ustreznost dodatne pravne podlage, tj. člena 16 PDEU, in uporaba protokolov št. 21 in 22 v okviru uporabe sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj (oddelek III).

II. USTREZNOST ČLENA 114 PDEU KOT PRAVNE PODLAGE

9. V skladu z ustaljeno sodno prakso pravna podlaga akta Unije ni odvisna od prepričanja institucije o tem, kaj je zastavljeni cilj, temveč jo je treba določiti na podlagi objektivnih meril, ki jih je mogoče sodno preskusiti, med temi pa sta zlasti cilj in vsebina ukrepa. Če se pri pregledu ukrepa izkaže, da ima ta dvojni namen ali vsebuje dva elementa, pri čemer je eden od obeh namenov oziroma elementov glavni ali prevladujoč, drugi pa zgolj postranski, mora ukrep imeti eno samo pravno podlago, in sicer tisto, ki jo zahteva glavni ali prevladujoči namen oziroma element. Izjemoma pa – če se ugotovi, da ima akt hkrati več ciljev, ki so neločljivo povezani in med njimi noben ni drugotnega in posrednega pomena v primerjavi z drugimi – lahko tak akt temelji na različnih ustreznih pravnih podlagah, razen če te pravne podlage predpisujejo postopke, ki med seboj niso združljivi. Poleg tega je treba opozoriti, da je v prvem stavku člena 114(1) PDEU jasno določeno, da se določbe člena uporabljajo, „[k]adar Pogodbi ne določata drugače“. Zato je uporaba člena 114 PDEU upravičena le, če za pravno podlago za sprejetje zadevnega ukrepa ni mogoče uporabiti nobene druge posebne določbe⁶. Če Pogodba vsebuje podrobnejšo določbo, ki je lahko pravna podlaga za zadevni ukrep, mora ukrep temeljiti na navedeni določbi⁷.

⁶ Mnenje pravne službe Sveta z dne 17. maja 2016, 9007/16, točka 6.

⁷ Sodba z dne 29. aprila 2004, *Komisija proti Svetu*, C-338/01, EU:C:2004:253, točka 60.

A. CILJ PREDLAGANE UREDBE

10. Predlagana uredba usklajuje dajanje na trg, dajanje v uporabo in uporabo določene vrste programske opreme (umetnointeligentnih sistemov). Dejstvo, da so lahko javni organi in zasebni subjekti ponudniki ali uporabniki takih umetnointeligentnih sistemov, samo po sebi ni nezdržljivo s členom 114 PDEU kot pravno podlago⁸.
11. Poleg tega dejstvo, da so lahko organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali tisti, ki delujejo v njihovem imenu, med ponudniki ali uporabniki takih umetnointeligentnih sistemov, ne zadostuje za utemeljitev za to, da se kot pravna podlaga uporabi člen 87 PDEU. Da bi ugotovili, ali je to potrebno, je treba analizirati cilj in vsebino predlagane uredbe.
12. Cilj predlagane uredbe je na splošno, tudi v zvezi s sistemi za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih in umetnointeligentnimi sistemi velikega tveganja, zagotoviti dosledno in visoko raven varstva po vsej Uniji, hkrati pa preprečiti, da bi razlike ovirale prosti pretok umetnointeligentnih sistemov ter z njimi povezanih proizvodov in storitev na notranjem trgu. V predlagani uredbi so določene enotne obveznosti za operaterje ter zagotavlja enotno varstvo prevladujočih razlogov javnega interesa in pravic oseb na celotnem notranjem trgu (uvodna izjava 2). Natančneje, določena so pravila, ki urejajo dajanje na trg in v uporabo nekaterih umetnointeligentnih sistemov, s čimer je zagotovljeno nemoteno delovanje notranjega trga in omogočeno, da ti sistemi izkoristijo načelo prostega pretoka blaga in storitev (uvodna izjava 5). Na splošno je namen predloga vzpostaviti že v zasnovi zaupanja vredno umetno inteligenco, ki bi se uporabljala na vseh področjih, s celovitim sklopom pravil za razvoj, trženje in uporabo proizvodov, storitev in sistemov, ki temeljijo na umetni inteligenci. Glede na to, da se je umetna inteligenca že vključila v številne storitve in proizvode ter da se bo vanje vključevala tudi v prihodnje, predlog sledi logiki notranjega trga, saj vzpostavlja „okvir za varnost proizvodov“, ki temelji na sklopu štirih kategorij tveganja. Določa zahteve za vstop na trg in certificiranje umetnointeligentnih sistemov velikega tveganja na podlagi obveznega postopka označevanja z oznako CE.

⁸ Glej pravno mnenje pravne službe Sveta (ST 11395/14, točke 39 do 41) in predhodne akte, kot so Direktiva (EU) 2016/2102 ter direktive 2014/24/EU, 2014/25/EU in 2014/23/EU.

13. Noben od navedenih ciljev predlagane uredbe se ne nanaša na zagotavljanje ciljev javne varnosti. Tudi če bi bilo treba cilje javne varnosti doseči posredno s postopkom harmonizacije dajanja na trg/dajanja v uporabo/uporabe umetnointeligenčnih sistemov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, je Sodišče⁹ pri razlagi člena 87(2) PDEU glede na člen 67 PDEU navedlo, da mora biti akt Unije, da bi ob upoštevanju svojega namena in vsebine temeljil na členu 87(2), neposredno povezan s cilji iz člena 67 PDEU (tj. v tem primeru s preprečevanjem kriminala in policijskim sodelovanjem). To je izključeno v okviru predlagane uredbe, saj so edina harmonizirana pravila o uporabi takih sistemov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj bodisi (1) standardna pravila o varnosti proizvodov, ki se enotno uporabljajo za vse ponudnike in uporabnike v zvezi z dajanjem na trg/dajanjem v uporabo ali uporabo umetnointeligenčnih sistemov, bodisi (2) pravila o varstvu osebnih podatkov, za katera je bila dodana pravna podlaga, ki jo predstavlja člen 16 PDEU (glej del III spodaj).
14. V drugi zadevi¹⁰, čeprav je bil cilj spremembe direktive o strelnem orožju zagotoviti višjo raven javne varnosti glede na grožnjo terorizma in drugih oblik kriminala, je Sodišče razsodilo, da je harmonizacija vidikov glede varnosti blaga eden od bistvenih elementov za zagotovitev pravilnega delovanja notranjega trga, saj bi lahko heterogeni predpisi na tem področju povzročili ovire pri trgovanju¹¹.

⁹ Sodba z dne 6. maja 2014, *Evropska komisija proti Evropskemu parlamentu in Svetu Evropske unije*, C-43/12, EU:C:2014:298.

¹⁰ Sodba z dne 3. decembra 2019, *Češka republika proti Evropskemu parlamentu in Svetu EU*, C-482/17, EU:C:2019:1035.

¹¹ Prav tam, točka 57: „Ker pa je posebnost strelnega orožja, v nasprotju s tem, kar trdi Republika Poljska, njihova nevarnost, in sicer ne le za uporabnike, temveč tudi za širšo javnost, kot je Sodišče že poudarilo v točki 54 sodbe z dne 23. januarja 2018, *Buhagiar in drugi* (C- 267/16, EU:C:2018:26), je upoštevanje javne varnosti, kot je opozorjeno v peti uvodni izjavi Direktive 91/477, v okviru zakonodaje o nabavi in posedovanju tega blaga očitno nepogrešljivo.“ Glej tudi sodbo z dne 23. januarja 2018, *Albert Buhagiar in drugi proti Minister for Justice*, C-267/16, EU:C:2018:26, točka 54: „V zvezi s tem je treba ugotoviti, da je glede na tveganje za varnost oseb, ki ga pomeni strelno orožje, njegov prosti pretok bilo mogoče doseči zgolj s strogim uokvirjenjem pogojev za njegov prenos med državami članicami, med katerimi je načelo predhodnega dovoljenja, ki ga izdajo države članice, ki jih prenos takšnega blaga zadeva.“

15. Cilji predlagane uredbe, vključno s členom 5(1)(d), (2), (3) in (4) o uporabi sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter določbami v zvezi z umetnointeligenčnimi sistemi velikega tveganja iz točke 6 Priloge III, niso neposredno povezani s ciljem javne varnosti. Nasprotno, predlog je odziv na glavne pomisleke v zvezi s tem, kako umetnointeligenčni sistemi vplivajo na zdravje, varnost in temeljne pravice. Zato so zadevne določbe neposredno povezane s ciljem zagotavljanja enakih konkurenčnih pogojev pri dajanju na trg/dajanju v uporabo ali uporabi umetnointeligenčnih sistemov na notranjem trgu ob hkratnem varovanju zdravja, varnosti in temeljnih pravic uporabnikov.
16. Glede na navedeno je glavni cilj predlagane uredbe izboljšati delovanje notranjega trga v smislu člena 114 PDEU, cilji iz člena 67 PDEU pa so le posredno in postransko povezani s tem glavnim ciljem.

B. VSEBINA PREDLAGANE UREDBE

17. Predlagana uredba v bistvu vsebuje pravila o tem, kaj je potrebno za to, da se določen proizvod (programska oprema umetne inteligence) da na trg (ali v uporabo) tako, da se zagotovi, da je varen in spoštuje temeljne pravice. Določa celovit sklop pravil za razvoj, trženje in uporabo proizvodov, storitev in sistemov, ki temeljijo na umetni inteligenci. Predlagana uredba niti ne zavezuje organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj k uporabi umetnointeligenčnega sistema, ki je zakonito dan na trg, niti ne ureja neposredno, kako bi morali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj uporabljati tak umetnointeligenčni sistem. Namesto tega jasno določa primere, v katerih se predvidena uporaba šteje za uporabo z velikim tveganjem zgolj zato, ker bodo umetnointeligenčni sistem uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali pravosodni organi.

18. Sicer pa člen 29 predlagane uredbe vsebuje pravila o pogojih za uporabo umetnointeligenčnih sistemov velikega tveganja, vendar taka določba ni specifična za sektor, ima omejeno področje uporabe (predvsem na navodila za uporabo proizvoda) in je neločljivo povezana z obveznostmi, ki jih imajo razvijalci umetnointeligenčnih sistemov v skladu s predlagano uredbo. Državam članicam daje tudi nekaj manevrskega prostora, da določijo nadaljnja pravila o uporabi takih umetnointeligenčnih sistemov velikega tveganja. Kar zadeva sisteme za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih, ki se uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (člen 5), predlagana uredba delno ureja uporabo takih sistemov z vidika varstva podatkov na podlagi člena 16 PDEU (glej del III spodaj).
19. Poleg tega se lahko samo države članice odločijo, da bodo zagotovile možnost, da v celoti ali delno dovolijo uporabo takih sistemov za biometrično identifikacijo na daljavo v realnem času. Posebne pogoje za tako uporabo je treba še določiti v nacionalni zakonodaji, vendar morajo upoštevati splošna merila in zaščitne ukrepe iz Uredbe: predhodno sodno ali upravno dovoljenje, zahtevo, izdajo in izvajanje predhodnega dovoljenja ter navedbo kaznivih dejanj, v zvezi s katerimi se taki sistemi lahko uporabljajo.

20. Umetnointeligenčni sistemi so posebna vrsta programske opreme. Harmonizirana pravila, ki se uporabljajo za dajanje umetnointeligenčnih sistemov na trg ali v uporabo ali za njihovo uporabo, so zato vrsta harmoniziranih pravil za varnost proizvodov. Uporabljajo se enotno brez razlikovanja med javnimi in zasebnimi uporabniki. V skladu z ustreznimi uvodnimi izjavami predlagane uredbe bi bilo zato treba zagotoviti dosledno in visoko raven varstva po vsej Uniji. Hkrati bi bilo treba preprečiti razlike, ki ovirajo prosti pretok umetnointeligenčnih sistemov ter z njimi povezanih proizvodov in storitev na notranjem trgu. To bi bilo doseženo z določitvijo enotnih obveznosti za operaterje ter zagotovitvijo enotnega varstva prevladujočih razlogov javnega interesa in pravic oseb na celotnem notranjem trgu na podlagi člena 114 PDEU¹².
21. Predlagana uredba vsebuje več sklicevanj na preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, upravljanje nadzora meja in upravljanje pravosodja v Prilogi III o umetnointeligenčnih sistemih velikega tveganja (točke 6, 7 oziroma 8). Ta vključujejo podroben in izčrpen seznam, ki ustreza členu 6(2), poleg drugih sistemov velikega tveganja v zvezi s tveganji za varnost proizvodov iz člena 6(1). V skladu s členom 6(1) je namreč treba nekatere umetnointeligenčne sisteme zaradi njihove pričakovane resnosti in velikih tveganj za temeljne pravice, zdravje in varnost že po definiciji šteti za sisteme velikega tveganja. Drugi sistemi, ki se štejejo za sisteme velikega tveganja in so navedeni v Prilogi III, vključujejo izobraževanje, upravljanje kritične infrastrukture, zaposlovanje, biometrično identifikacijo in kategorizacijo ter dostop do bistvenih javnih in zasebnih storitev.

¹² Zato je potreben pravni okvir Unije, ki bo določal harmonizirana pravila o umetni inteligenci, da bi spodbudil razvoj, uporabo in uvajanje umetne inteligence na notranjem trgu, ki bo hkrati zagotavljal visoko raven zaščite javnih interesov, kot so zdravje in varnost ter varstvo temeljnih pravic, kot jih priznava in varuje pravo Unije. Za doseg tega cilja bi bilo treba določiti pravila, ki urejajo dajanje na trg in v uporabo nekaterih umetnointeligenčnih sistemov, s čimer bi zagotovili nemoteno delovanje notranjega trga in omogočili, da ti sistemi izkoristijo načelo prostega pretoka blaga in storitev (glej uvodni izjavi 2 in 5 predloga).

22. Vendar taka pravila o umetnointeligenčnih sistemih velikega tveganja ne določajo, ali bi morali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in pravosodni organi (ali organi na drugih opredeljenih področjih) uporabljati te sisteme ali ne. Predlagana uredba bo le posredno vplivala na dejanski razvoj umetnointeligenčnih sistemov, ki bi jih lahko uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ter na umetnointeligenčne sisteme, ki se uporabljajo trenutno in se bodo uporabljali v prihodnosti. Pravila se torej nanašajo na umetnointeligenčne sisteme, ki naj bi jih ti organi „predvidoma uporabljali“ (glej npr. člen 3(12), člen 8(2) in Prilogo III). Posledica razvrstitve določenega umetnointeligenčnega sistema kot sistema velikega tveganja je uporaba posebnega sklopa pravil o obvladovanju tveganja, upravljanju podatkov in tehničnih specifikacijah. Uporabniki takih umetnointeligenčnih sistemov velikega tveganja morajo upoštevati navodila za uporabo, voditi dnevnike in izvajati ocene učinka v zvezi z varstvom podatkov.
23. Poleg tega se lahko obveznosti uporabnikov, ki niso povezane z navodili za uporabo, določijo v pravu Unije ali nacionalnem pravu in brez poseganja v pravico uporabnika, da organizira lastna sredstva in dejavnosti za izvajanje ukrepov za človekov nadzor, ki jih navede ponudnik (člen 29(2) predlagane uredbe). Ta pravila določajo nadaljnje zaščitne ukrepe za temeljne pravice za umetnointeligenčne sisteme velikega tveganja.

24. Glede na navedeno je treba poudariti, da predlagana uredba ne vsebuje pravil, katerih cilj je organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj dovoliti ali preprečiti uporabo umetnointeligenčnega sistema velikega tveganja, danega na trg. Na podlagi predlaganih pravil se bo za umetnointeligenčni sistem, ki ga razvijejo ali uporabljajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, zaradi njegove predvidene uporabe uporabljala posebna oznaka (veliko tveganje). To uporabo bi urejalo nacionalno pravo, v določenem obsegu pa bi o njej odločali sami organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Predlagana uredba namreč v členu 29 določa minimalne pogoje za uporabo (omejene na navodila za uporabo) umetnointeligenčnih sistemov velikega tveganja, vključno s tistimi iz točk 6, 7 in 8 Priloge III, ki bodo dopolnjeni z nacionalnim pravom. Zato bi bilo treba v skladu s sodno prakso Sodišča razlikovati med, na eni strani, predvidenim ciljem predlagane uredbe, ki ni ureditev uporabe umetnointeligenčnih sistemov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ter, na drugi strani, učinki, ki jih lahko posredno povzroči¹³ in ki niso pomembni za namene analize ustreznosti pravne podlage.
25. Točke 6, 7 in 8 (o preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, migracijah in upravljanju pravosodja) ne prevladujejo med umetnointeligenčnimi sistemi velikega tveganja. V skladu s predlagano uredbo namreč umetnointeligenčni sistem velikega tveganja ni nujno sistem, ki je naveden v Prilogi III. Večina sistemov velikega tveganja je dejansko tistih, ki so na splošno navedeni v členu 6(1)(a) in (b) predlagane uredbe (v zvezi z varnostjo proizvodov). Drugi umetnointeligenčni sistemi velikega tveganja so navedeni v Prilogi III, ki vsebuje točke 1 (biometrična identifikacija), 2 (kritična infrastruktura), 3 (izobraževanje in poklicno usposabljanje) in 4 (zaposlovanje, upravljanje delavcev in dostop do samozaposlitve), ki se nanašajo na področja, ki niso področje pravosodja in notranjih zadev (v nadaljnjem besedilu: PNZ). Za vse uporabnike takih umetnointeligenčnih sistemov velikega tveganja velja enotna ureditev, ki ni določena glede na njihov posebni status (na primer, ali so gospodarski subjekt ali javni organ), temveč z vidika varovanja zdravja, varnosti in temeljnih pravic.

¹³ Glej sodbo Sodišča z dne 21. junija 2018, *Republika Poljska/Evropski parlament, Svet Evropske unije*, C-5/16, EU:C:2018:483, točke 63 do 68, in sodbo Sodišča z dne 22. junija 2022, *Leistritz AG proti LH*, C-534/20, EU:C:2022:495, točka 28.

26. Predlagana uredba tako vsebuje harmonizirana pravila o dajanju na trg, dajanju v uporabo in uporabi umetnointeligenčnih sistemov ne glede na to, ali jih uporabljajo zasebni subjekti ali javni organi, vključno in postransko¹⁴ z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in pravosodnimi organi.
27. Razen uporabe sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, za katero veljajo posebna pravila o obdelavi osebnih podatkov (glej del III spodaj), predlagana uredba ne vsebuje harmoniziranih pravil o uporabi umetnointeligenčnih sistemov velikega tveganja. Kot je pojasnjeno v točkah 18 in 19 zgoraj, se sklicevanje na uporabo umetnointeligenčnih sistemov velikega tveganja v bistvu nanaša na navodila za uporabo proizvoda (člen 29) in je povezano z obveznostmi razvijalcev. Kot je poudarjeno v točki 22, odločitev o tem, ali lahko organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali pravosodni organi uporabljajo umetnointeligenčni sistem velikega tveganja, ki je zakonito dan na trg v skladu s predlagano uredbo, ureja nacionalno pravo in jo sprejmejo nacionalni organi.
28. Zato člen 87(2) PDEU, zlasti točka (a) navedenega člena, ni ustrezna pravna podlaga za predlagano uredbo. Pravila v predlogu niti ne spodbujajo niti ne ovirajo zbiranja, shranjevanja, obdelave, analize in izmenjave ustreznih informacij. Povedano preprosto, kadar take dejavnosti izvajajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, bo treba upoštevati številne nespecifične in harmonizirane pogoje, da se zaščitijo pravice uporabnikov. Podobno navedeni cilji predlagane uredbe ne vključujejo razvoja skupnih preiskovalnih tehnik. Predlagane zahteve glede uporabe umetnointeligenčnih sistemov velikega tveganja niso specifične za področje PNZ in se ne nanašajo na policijsko sodelovanje *stricto sensu*, kot je opredeljeno v PDEU.

¹⁴ Glej mnenje Sodišča o *Istanbulski konvenciji*, A-1/19, EU:C:2021:198, zlasti točki 298 in 301.

29. V skladu z določbami člena 5(4) predlagane uredbe se lahko država članica še vedno odloči, da dovoli uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Če se odloči tako, mora določiti potrebna podrobna pravila za zahtevo, izdajo in izvajanje predhodnega dovoljenja ter s tem povezana kazniva dejanja, za preiskavo ali pregon katerih je uporaba dovoljena¹⁵. Na podlagi izida razprav v Svetu ta predlagana pravila ne bi privedla do podelitve novih pooblastil zadevnim nacionalnim organom. Namesto tega je uporaba obstoječih ali morebitnih prihodnjih mehanizmov omejena, da se zagotovi varstvo pravice do zasebnosti in osebnih podatkov.
30. Glede na navedeno je člen 114 PDEU edina ustrezna pravna podlaga za harmonizirana pravila o umetnointeligenčnih sistemih velikega tveganja, vključno s tistimi, ki jih uporabljajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in pravosodni organi, katera koli pravna podlaga s področja PNZ iz naslova V tretjega dela PDEU, kot je člen 87 PDEU, v zvezi s temi harmoniziranimi pravili pa ni niti upravičena niti ustrezna.

¹⁵ Omeniti je treba, da ima člen 5(4) predloga nekatere značilnosti, podobne členu 15(1) Direktive 2002/58/ES o elektronskem poslovanju. Zlasti določa možnost, da države članice odstopajo od nekaterih prepovedi, določenih v pravu Unije. Glede na ustaljeno sodno prakso bodo nacionalne določbe, katerih namen je odstopanje od navedene prepovedi, nujno spadale v področje uporabe prava Unije, kar bo posledično sprožilo uporabo Listine v zvezi z njimi.

III. USTREZNOST ČLENA 16 PDEU KOT DODATNE PRAVNE PODLAGE

31. Predlagana uredba vključuje člen 16 PDEU kot pravno podlago v zvezi z obdelavo osebnih podatkov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, uvodni izjavi 25 in 26 pa vključujeta sklicevanje na člen 6a Protokola št. 21 in člen 2a Protokola št. 22 o obdelavi osebnih podatkov na področju preprečevanja kriminala. Po mnenju Komisije naj bi se člen 16 PDEU uporabljal izključno kot pravna podlaga za določbe, ki dodatno omejujejo obdelavo biometričnih osebnih podatkov v primerjavi z Direktivo 2016/680 (v nadaljnjem besedilu: direktiva o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj). Člen 5(1)(c) je oblikovan kot načelna prepoved, za katero veljajo tri izjeme. Konkretno, uporaba sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj je prepovedana, razen če je nujno potrebna za (a) izvajanje usmerjenih iskanj potencialnih žrtev kaznivih dejanj, (b) preprečitev neposrednega terorističnega napada ali napada na telesno nedotakljivost/življenje osebe, (c) lokalizacijo ali identifikacijo ali pregon storilca ali osumljenca hudega kaznivega dejanja (s sklicevanjem na evropski nalog za prijetje). Dodatne zahteve iz člena 5(2), (3) in (4) so povezane s to posebno uporabo umetnointeligenčnih sistemov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, zlasti ocena nujnosti in sorazmernosti, predhodno dovoljenje (razen v izrednih razmerah) in odločitev držav članic, ali bodo na nacionalni ravni dovolile posebno uporabo orodij umetne inteligence v takih primerih ali ne.
32. Člen 5 je podrobna določba, ki ureja posebno uporabo orodij umetne inteligence in ki je ne le namenjena dopolnitvi veljavnega zakonodajnega okvira Unije (direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, ki sama temelji na členu 16 PDEU), temveč zahteva tudi nacionalni okvir za izvajanje.

33. V bistvu je mogoče posebno pravilo iz člena 5, čeprav je oblikovano kot prepoved, opisati tako, da določa strog in izjemen okvir splošnega spremljanja posameznikov v odprtih prostorih v realnem času, ki se izvaja z instrumenti umetne inteligence z namenom njihove identifikacije. Prepoved tudi presega preprosto uporabo kamer za snemanje in se nanaša na uporabo orodij umetne inteligence za samodejno prepoznavanje človeških značilnosti v javno dostopnih prostorih (značilnosti, kot so obrazi, pa tudi način hoje, prstni odtisi, DNK, glas, udarci na tipke in drugi biometrični ali vedenjski znaki). Vključuje tudi sočasno zajemanje in identifikacijo oseb z analizo primerjavo/preverjanjem podatkov. Poleg tega je treba pravilo presojati tudi ob upoštevanju dejstva, da se lahko identifikacija zasebnih uporabnikov na javnih mestih v realnem času tudi dovoli (za dogodke, kot so nogometne tekme).
34. Zdi se, da dodatna pojasnila, ki jih je predložila Komisija, kažejo, da ni trenutno nobena država članica uredila tega specifičnega vprašanja oziroma ga je uredilo le zelo malo držav članic, da bi organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj omogočili uporabo orodij umetne inteligence pri odkrivanju posameznikov na javnih mestih v realnem času. Vendar čeprav v praksi niso bili predloženi trdni dokazi, ki bi dokazovali, da bo treba obstoječe prakse in orodja spremeniti, se zdi jasno, da bodo morali prihodnje preiskovalne tehnike, forenzične metode in pravila o zbiranju dokazov vključevati ta pristop prepovedi/izjem.
35. Kar zadeva pravno podlago, se zdi, da določbe, ki dodatno omejujejo obdelavo biometričnih osebnih podatkov (v primerjavi z direktivo o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj), sledijo cilju varstva osebnih podatkov z določitvijo ustreznih zaščitnih ukrepov. Tak cilj je neločljivo povezan s ciljem določb, ki spadajo v področje uporabe člena 114 PDEU, pri čemer ni nobena drugotnega ali posrednega pomena glede na drugo. Cilj predlagane uredbe je določiti splošen okvir za umetnointeligenčne sisteme na podlagi pristopa, ki temelji na tveganju. V tem okviru lahko horizontalna ureditev umetnointeligenčnih sistemov vključuje stroge zaščitne ukrepe, ki se uporabljajo za ta posebni umetnointeligenčni sistem odkrivanja v realnem času. Tak posebni umetnointeligenčni sistem, ki vsebuje ustrezne zaščitne ukrepe za varstvo osebnih podatkov, je torej neločljivo povezan s splošnim ciljem izboljšanja delovanja notranjega trga in ni drugotnega ali posrednega pomena glede na slednjega. Predlagana uredba bi zato morala temeljiti na dveh podlagah v skladu z ustrežno sodno prakso (glej točko 9 zgoraj).

36. Vendar ostaja vprašanje, katero pravno podlago bi bilo treba uporabiti za urejanje obdelave osebnih podatkov za uporabo sistemov iz člena 5(1)(c) do (4) predlagane uredbe.
- Člen 87(2)(a) PDEU je namreč pravna podlaga za ukrepe služb kazenskega pregona v zvezi s preprečevanjem, odkrivanjem in preiskovanjem kaznivih dejanj glede zbiranja, hrambe, obdelave, analize in izmenjave koristnih informacij.
37. Kot je generalni pravobranilec pojasnil v sklepnih predlogih o PNR Kanada (A1/15), med členom 16 PDEU na eni strani ter členoma 87(2)(a) PDEU in 82(1)(d) PDEU na drugi strani niso mogoča hierarhična razmerja „*lex generalis – lex specialis*“¹⁶. Člen 16(2) PDEU je edina določba, ki se uporablja za pravila o varstvu posameznikov pri obdelavi osebnih podatkov s strani organov držav članic za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj pri izvajanju dejavnosti za preprečevanje kriminala. Zgolj dejstvo, da se člen 5 sklicuje na seznam hudih kaznivih dejanj v okvirnem sklepu o evropskem nalogu za prijetje, ne spremeni te ocene: to sklicevanje ne pomeni, da se navedeni okvirni sklep uporablja kot tak¹⁷. Je zgolj zakonodajna tehnika za navedbo seznama kaznivih dejanj, ne da bi bilo treba oblikovati ločeno prilogo.
38. Dejstvo ostaja, da je pravilo iz člena 5 določeno ne kot sredstvo za nadaljnjo razmejitev pogojev uporabe teh ukrepov, povezanih s PNZ, temveč z namenom zagotovitve, da se bodo v prihodnje pri vsaki uporabi biometrične identifikacije v realnem času z umetnointeligentnimi sistemi ustrezno upoštevali pomisleki v zvezi s temeljnimi pravicami in predvsem potreba po zagotovitvi, da se biometrični podatki zbirajo in obdelujejo ob spoštovanju pravice do zasebnosti in osebnih podatkov.

V zvezi s tem Uredba ni namenjena določitvi novega, obveznega postopka, specifičnega za PNZ, temveč se opira na preizkušena in preverjena postopkovna sredstva za zagotovitev spoštovanja temeljnih pravic.

¹⁶ Glej sklepne predloge generalnega pravobranilca P. Mengozzija z dne 8. septembra 2016, *Osnutek sporazuma med Kanado in Evropsko unijo*, Mnenje 1/15, EU:C:2016:656, točke 112 do 120.

¹⁷ V zvezi z izvajanjem tega seznama hudih kaznivih dejanj v državah članicah glej sodbo Sodišča z dne 21. junija 2022, *Ligue des droits humains proti Conseil des ministres*, C-817/19, EU:C:2022:65, točke 150 do 152.

39. Če je člen 16 PDEU ustrezna dodatna pravna podlaga, se postavljajo vprašanja glede uporabe členov 6a in 2a Protokola št. 21 oziroma Protokola št. 22. Kot je pojasnjeno v uvodnih izjavah 25 in 26 predloga, to pomeni, da kadar organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj na Irskem ali Danskem uporabljajo sisteme za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za preprečevanje kriminala in če Irske ali Danske ne zavezujejo ustrezna pravila o policijskem ali pravosodnem sodelovanju v kazenskih zadevah, člen 5(1)(d), (2) in (3) predlagane uredbe ni zavezujoč za ti državi članici. To ne pomeni, da člen 5(1)(d), (2) in (3) vsebuje pravila o policijskem sodelovanju, kot so pravila o izmenjavi informacij med organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. To preprosto pomeni, da člen 5(1)(d), (2) in (3) predlagane uredbe podobno kot Direktiva 2016/680 (direktiva o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj), ki je *lex generalis*, sprejeta na podlagi člena 16 PDEU, ureja obdelavo biometričnih osebnih podatkov v posebnem okviru sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za preprečevanje kriminala in nič več. Predlog Komisije v zvezi s tem sledi pristopu, ki ga je zakonodajalec Unije uporabil za direktivo o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, in kot tak potrjuje, da uporaba člena 87(2) PDEU v tem okviru ni upravičena.
40. Dodatek člena 16 PDEU k členu 114 PDEU je v tem primeru upravičen z dejstvom, da člen 5(1)(d), (2) in (3) določa edine dovoljene primere urejanja uporabe umetnointeligenčnega sistema, ki posega v pravico do varstva osebnih podatkov, kar je *lex specialis* glede na splošni okvir varstva podatkov. Takih pravil *lex specialis* o varstvu podatkov, ki vplivajo na uporabo navedenih občutljivih umetnointeligenčnih sistemov, ni mogoče šteti za drugotna ali posredna glede na pravno podlago notranjega trga. Zato je vključitev člena 16 PDEU kot pravne podlage v predlagani uredbi zadostno utemeljena, uporaba člena 87(2)(a) PDEU pa ni ustrezna.

IV. ZAKLJUČEK

41. Glede na navedeno pravna služba Sveta meni, da:

- a) je uporaba členov 16 in 114 PDEU kot pravnih podlag za predlagano uredbo upravičena in ustrezna;
 - b) uporaba člena 87(2) PDEU ali katere koli druge pravne podlage s področja PNZ ni upravičena ali ustrezna v zvezi s harmoniziranimi pravili, ki se uporabljajo za umetnointeligenčne sisteme, ki jih lahko zagotovijo ali uporabljajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali pravosodni organi.
-