EUROPSKA
KOMISIJA

Bruxelles, 20.5.2026.
COM(2026) 234 final

IZVJEŠĆE KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

IZVJEŠĆE DONESENO NA TEMELJU ČLANKA 112. STAVKA 1. UREDBE (EU) 2024/1689 O POTREBI ZA PREISPITIVANJEM POPISA ZABRANJENIH PRAKSI U PODRUČJU UMJETNE INTELIGENCIJE I VISOKORIZIČNIH UI SUSTAVA NAVEDENIH U PRILOGU III.

IZVJEŠĆE KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

IZVJEŠĆE DONESENO NA TEMELJU ČLANKA 112. STAVKA 1. UREDBE (EU) 2024/1689 O POTREBI ZA PREISPITIVANJEM POPISA ZABRANJENIH PRAKSI U PODRUČJU UMJETNE INTELIGENCIJE I VISOKORIZIČNIH UI SUSTAVA NAVEDENIH U PRILOGU III.

1. Kontekst i osnovne informacije

(1) Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni određenih uredaba („UI akt”[1]) stupila je na snagu 1. kolovoza 2024. Tom se uredbom utvrđuje sveobuhvatan pravni okvir za regulaciju umjetne inteligencije („UI”) u Uniji, a cilj joj je promicanje inovacija i uvođenja umjetne inteligencije uz istodobno osiguravanje visoke razine zaštite zdravlja, sigurnosti i temeljnih prava u Europskoj uniji, uključujući demokraciju i vladavinu prava.

(2) UI akt slijedi pristup koji se temelji na procjeni rizika, pri čemu se sustavi umjetne inteligencije („UI sustavi”) klasificiraju u četiri kategorije: (i) neprihvatljiv rizik, (ii) visok rizik, (iii) rizik u pogledu transparentnosti i (iv) minimalan ili nikakav rizik. Kad je riječ o kategoriji neprihvatljivog rizika, u UI aktu navode se konkretne prakse u području umjetne inteligencije koje su zabranjene u EU-u (članak 5. UI akta). UI sustavi klasificirani su kao visokorizični u skladu s člankom 6. UI akta, u vezi s Prilogom I. (popis zakonodavstvenih akata Unije o usklađivanju) i Prilogom III. UI aktu. Prilog III. obuhvaća osam područja te se u njemu navode konkretni primjeri upotrebe za svako područje za koje su Europski parlament i Vijeće procijenili da predstavljaju visok rizik od štete za zdravlje i sigurnost osoba ili za temeljna prava.

(3) UI akt osmišljen je kao fleksibilan pravni instrument koji će se moći prilagođavati budućim potrebama i koji omogućuje prilagodbu određenih pravila brzom tehnološkom razvoju, kao i mogućim promjenama u upotrebi UI sustava i novim rizicima. Zbog toga su UI aktom predviđeni stalno praćenje i revizija, čime se postiže da pravila ostanu relevantna i djelotvorna. To se primjenjuje čak i prije početka primjene određenih odredaba, kao što su pravila za visokorizične UI sustave.

(4) Člankom 112. UI akta predviđen je poseban instrument za praćenje radi evaluacije i preispitivanja UI akta. U skladu s člankom 112 stavkom 1. Komisija je jednom godišnje nakon stupanja na snagu UI akta i do kraja razdoblja delegiranja ovlasti utvrđenog u članku 97. dužna procijeniti potrebu za izmjenom popisa visokorizičnih UI sustava iz Priloga III. i popisa zabranjenih praksi u području umjetne inteligencije utvrđenog u članku 5. UI akta. Komisija zaključke te procjene mora podnijeti Europskom parlamentu i Vijeću.

(5) Ovo je prvo izvješće doneseno na temelju te odredbe. Cilj mu je procijeniti postoji li potreba za izmjenom popisa primjera upotrebe iz Priloga III. i popisa zabranjenih praksi u području umjetne inteligencije iz članka 5. UI akta, kako bi se osiguralo da UI akt ostane

[1] Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024.).

relevantan i djelotvoran usprkos brzom razvoju tehnologija umjetne inteligencije. Ovo izvješće ne obuhvaća preispitivanje popisa područja iz Priloga III. jer je Komisija to preispitivanje dužna provesti do 2. kolovoza 2028., u skladu s člankom 112. stavkom 2. UI akta.

(6) Na početku ovog izvješća predstavljena je metodologija korištena u njegovoj pripremi. Zatim se ta metodologija primjenjuje kako bi se predstavila procjena moguće potrebe za preispitivanjem popisa primjera visokorizične upotrebe iz Priloga III. i popisa zabranjenih praksi u području umjetne inteligencije iz članka 5. UI akta.

(7) Procjena u ovom izvješću ograničena je kratkim razdobljem koje je proteklo od stupanja na snagu UI akta i njegovom kratkom primjenom u trenutku donošenja ovog izvješća. Poglavlje II. UI akta (Zabranjene prakse) počelo se primjenjivati 2. veljače 2025. Međutim, pravila o izvršavanju tog poglavlja primjenjivat će se tek od 2. kolovoza 2026., a nacionalna nadležna tijela još su u postupku imenovanja. Obveze koje se odnose na visokorizične UI sustave iz Priloga III. UI aktu primjenjivat će se od 2. kolovoza 2026., a razmatra se i produljenje[2]. Nadalje, premda su smjernice Komisije o zabranjenim praksama u području umjetne inteligencije objavljene u veljači 2025.[3], smjernice o klasifikaciji visokorizičnih UI sustava još su u pripremi. Stoga u tim smjernicama tek treba pojasniti određene koncepte i klasifikaciju određenih primjera upotrebe umjetne inteligencije te ih dodatno razraditi praktičnom primjenom Priloga III. UI aktu i povezanih odredaba.

2. Metodologija primijenjena za preispitivanje na temelju članka 112. stavka 1. UI akta

(8) Radi usmjeravanja evaluacija i preispitivanja iz članka 112. stavka 1. UI akta, Ured za umjetnu inteligenciju trebao bi, u skladu s člankom 112. stavkom 11., razviti objektivnu i participativnu metodologiju za evaluaciju razina rizika na temelju kriterija navedenih u relevantnim člancima i za uključivanje novih sustava na popis iz Priloga III., uključujući proširenje postojećih kategorija područja ili dodavanje novih kategorija područja u taj prilog, te na popis zabranjenih praksi iz članka 5. UI akta.

(9) U ovom odjeljku izvješća predstavljen je metodološki pristup koji je Ured za umjetnu inteligenciju razvio kako bi priprema ovog izvješća bila u skladu s tom obvezom. Prvo, u njemu se daje pregled pravnih kriterija za preispitivanje popisa zabranjenih praksi u području umjetne inteligencije iz članka 5. UI akta i popisa visokorizičnih UI sustava iz Priloga III. (odjeljak 2.1. u nastavku). Ti pravni kriteriji temelj su za daljnju procjenu potrebe za preispitivanjem, posebno u pogledu konkretnih UI sustava koji mogu biti obuhvaćeni tim dvjema kategorijama. Drugo, u izvješću se opisuju participativne metode

[2] Komisija je u Digitalnom omnibusu o umjetnoj inteligenciji predložila da se vremenski okvir provedbe pravila za visokorizične UI sustave poveže s dostupnošću normi i drugih instrumenata za potporu. Nakon što Komisija potvrdi da su te norme i instrumenti dostupni, pravila će se početi primjenjivati nakon šestomjesečnog prijelaznog razdoblja za visokorizične UI sustave iz Priloga III., a u svakom slučaju najkasnije 2. prosinca 2027. O tome se i dalje pregovara i predmet je dogovora između Europskog parlamenta i Vijeća. Više pojedinosti potražiti u Prijedlogu uredbe Europskog parlamenta i Vijeća o izmjeni uredaba (EU) 2024/1689 i (EU) 2018/1139 u pogledu pojednostavnjenja provedbe usklađenih pravila o umjetnoj inteligenciji (Digitalni omnibus o umjetnoj inteligenciji). {SWD(2025) 836 final}, Bruxelles, 19.11.2025., COM(2025) 836 final, 2025/0359 (COD).

[3] Dostupno na: Komisija objavljuje Smjernice o zabranjenim praksama u području umjetne inteligencije, kako su definirane Aktom o umjetnoj inteligenciji. | Izgradnja digitalne budućnosti Europe

korištene za prikupljanje i analizu dokaza te pristup koji se primjenjivao u cijelom postupku procjene (odjeljak 2.2. u nastavku).

2.1. Pravni kriteriji za procjenu potrebe za izmjenom popisa zabranjenih praksi u području umjetne inteligencije iz članka 5. UI akta i popisa primjera visokorizične upotrebe iz Priloga III. UI aktu

(10) Procjena potrebe za izmjenom popisa zabranjenih praksi u području umjetne inteligencije iz članka 5. UI akta, kao i primjera visokorizične upotrebe iz Priloga III. UI aktu, temelji se na pravnim kriterijima. Kad je riječ o Prilogu III. UI aktu, ti su kriteriji izričito navedeni u samom Aktu (članak 7.), a kad je riječ o članku 5. Akta, izvedeni su iz temeljnih načela zakonodavstva.

2.1.1. Kriteriji za preispitivanje popisa zabrana iz članka 5.

(11) Člankom 5. UI akta zabranjuje se stavljanje na tržište EU-a, stavljanje u upotrebu ili korištenje određenog broja UI sustava za manipulativne i izrabljivačke prakse, prakse društvene kontrole i nadzora te druge prakse, koje same po sebi krše temeljna prava i vrijednosti EU-a. U uvodnoj izjavi 28. UI akta pojašnjava se da su takve prakse osobito štetne i predstavljaju zlouporabu jer su u suprotnosti s vrijednostima EU-a kojima se poštuju ljudsko dostojanstvo, sloboda, jednakost, demokracija i vladavina prava te temeljna prava zajamčena Poveljom EU-a o temeljnim pravima („Povelja”)[4]. Stoga bi preispitivanje članka 5. UI akta moglo biti opravdano kad god dostatni dokazi upućuju na to da se trenutačnim zabranama na odgovarajući način ne uzimaju u obzir nove ili novonastajuće prakse u području umjetne inteligencije kojima se stvarno ugrožavaju vrijednosti EU-a ili temeljna prava utvrđena u Povelji i koje se smatraju osobito štetnima te predstavljaju zlouporabu.

(12) Nadalje, člankom 5. stavkom 8. UI akta predviđeno je da UI akt ne utječe na postojeće zabrane na temelju drugih propisa EU-a. Tom se odredbom naglašava međudjelovanje UI akta i drugih pravnih okvira zbog njegove horizontalne prirode[5]. Općenito, zabrane iz UI akta prvenstveno obuhvaćaju nedostatke koji već nisu predmet drugih propisa EU-a i za koje su potrebna tržišna pravila specifična za umjetnu inteligenciju. Međutim, premda se drugi pravni akti EU-a mogu usporedno primjenjivati, oni neizbježno pristupaju pitanjima iz drugih kutova, s drugačijim mehanizmima izvršavanja, te stoga možda ne uzimaju u dovoljnoj mjeri u obzir ukupne rizike određenih neprihvatljivih praksi u području umjetne inteligencije.

(13) Stoga Komisija preispituje popis zabranjenih praksi u području umjetne inteligencije iz članka 5. UI akta tako da procjenjuje potrebu za preispitivanjem, za koju trebaju biti ispunjena barem dva kumulativna uvjeta:

[4] Povelja Europske unije o temeljnim pravima. SL C 326, 26.10.2012., str. 391.

[5] Vidjeti u tom pogledu odjeljke 2.8., 3.6., 4.4., 5.4., 6.4. i 8.4. Smjernica o zabranjenim praksama u području umjetne inteligencije.

- postoje nove ili novonastajuće prakse u području umjetne inteligencije koje ugrožavaju vrijednosti EU-a ili prava i slobode iz Povelje, a koje nisu obuhvaćene trenutačnim popisom zabranjenih praksi iz članka 5. UI akta i
- unatoč drugim primjenjivim propisima EU-a i dalje postoje regulatorni nedostaci pa je potrebno preispitati zabrane iz UI akta kako bi štetne prakse u području umjetne inteligencije bile u potpunosti obuhvaćene.

(14) Članak 5. može se izmijeniti samo zakonodavnom izmjenom. Stoga, ako se utvrdi potreba za izmjenom članka 5. UI akta, Komisija će rezultate procjene dostaviti Europskom parlamentu i Vijeću te će razmotriti je li u tu svrhu potrebno predstaviti zakonodavni prijedlog.

2.1.2. Kriteriji za preispitivanje popisa visokorizičnih UI sustava iz Priloga III.

(15) Članak 6. UI akta, u vezi s prilozima I. i III., odnosi se na određene upotrebe UI sustava koji su klasificirani kao visokorizični zbog znatnog rizika od štete za zdravlje i sigurnost ili temeljna prava pojedinaca. Visokorizični UI sustavi trebali bi se stavljati na tržište Unije, stavljati u upotrebu ili koristiti samo ako ispunjavaju određene obvezne zahtjeve iz UI akta čiji je cilj otklanjanje tih rizika.

Ograničenje preispitivanja na primjere upotrebe visokorizičnih UI sustava iz Priloga III.

(16) U UI aktu razlikuju se dvije kategorije UI sustava koji su klasificirani kao „visokorizični" kako je utvrđeno u članku 6. stavcima 1. i 2. Akta. Prva su kategorija UI sustavi koji su ugrađeni kao sigurnosne komponente u proizvode ili koji su sami po sebi proizvodi obuhvaćeni zakonodavstvom EU-a o usklađivanju iz Priloga I., a koji bi mogli negativno utjecati na zdravlje i sigurnost pojedinaca te se stoga klasificiraju kao visokorizični u skladu s člankom 6. stavkom 1. UI akta. Druga kategorija obuhvaća UI sustave za koje se, s obzirom na njihovu namjenu, smatra da predstavljaju znatan rizik za zdravlje, sigurnost ili temeljna prava te se stoga klasificiraju kao visokorizični u skladu s člankom 6. stavkom 2. UI akta.

(17) Budući da se u članku 112. stavku 1. UI akta navodi moguća potreba za preispitivanjem primjera visokorizične upotrebe navedenih u Prilogu III., ovim izvješćem nisu obuhvaćeni UI sustavi koji su sigurnosne komponente proizvoda ili koji su sami po sebi proizvodi, a obuhvaćeni su područjem primjene određenog zakonodavstva EU-a o usklađivanju iz Priloga I. Upućivanje na visokorizične UI sustave u ovom izvješću odnosi se samo na samostalne UI sustave[6] koji su obuhvaćeni unaprijed definiranim područjima iz Priloga III.

Kriteriji za izmjenu primjera upotrebe visokorizičnih UI sustava navedeni u članku 7.

(18) Na temelju članka 7. UI akta Komisija ima ovlast da delegiranim aktima izmijeni Prilog III. dodavanjem, izmjenom ili brisanjem primjera upotrebe visokorizičnih UI sustava kako bi se uzeo u obzir brz tempo tehnološkog razvoja, kao i moguće promjene u upotrebi UI sustava (vidjeti i uvodnu izjavu 52. i uvodnu izjavu 173. UI akta). Uvjeti za tu ovlast utvrđeni su u članku 7. stavcima od 1. do 3. UI akta.

[6] Visokorizični UI sustavi koji nisu sigurnosne komponente proizvoda ili koji su sami po sebi proizvodi klasificirani kao visokorizični na temelju članka 6. stavka 1.

(19) Prvo, u članku 7. stavku 1. UI akta utvrđeno je da Komisija može donijeti delegirane akte kako bi dodala nove primjere upotrebe u Prilog III. ili prilagodila one koji su trenutačno navedeni u tom prilogu pod uvjetom (i) da su UI sustavi namijenjeni korištenju u jednom od osam područja navedenih u Prilogu III. i (ii) da postoji rizik od štete koji je jednakovrijedan ili veći od već navedenih. Tim drugim uvjetom utvrđuje se prag za usporednu procjenu rizika: jedan od ključnih uvjeta za uvrštavanje dodatnih primjera upotrebe visokorizičnih UI sustava na popis jest da oni moraju predstavljati rizik za zdravlje i sigurnost ili temeljna prava pojedinaca koji je jednakovrijedan onima koji su već navedeni u Prilogu III. Time se postiže dosljednost i proporcionalnost u klasifikaciji visokorizičnih UI sustava.

(20) U članku 7. stavku 2. navode se kriteriji koji se moraju uzeti u obzir pri utvrđivanju je li taj prag dosegnut. Oni, među ostalim, uključuju namjenu UI sustava, stupanj u kojem će se vjerojatno upotrebljavati, prirodu obrađenih podataka te trenutačne i potencijalne razmjere štete. U uvodnoj izjavi 52. razjašnjen je temelj tih kriterija te je navedeno da je primjereno klasificirati samostalne UI sustave kao visokorizične ako, s obzirom na njihovu namjenu, kod njih postoji visok rizik od štete za zdravlje i sigurnost ili temeljna prava pojedinaca, uzimajući u obzir i težinu moguće štete i njezinu vjerojatnost nastanka, te ako se upotrebljavaju u nekoliko posebno unaprijed definiranih područja navedenih u UI aktu. Komisija ima određene diskrecijske ovlasti u primjeni kriterija, pod uvjetom da se na odgovarajući način uzmu u obzir i smatraju ispunjenima u ukupnoj procjeni.

(21) Stoga prag za izmjenu popisa iz Priloga III. UI aktu nije samo tehnološka novost ili zabrinutost javnosti, nego i dokaziv i usporediv rizik koji UI sustavi predstavljaju za zdravlje, sigurnost ili temeljna prava, sličan riziku koji predstavljaju UI sustavi koji su trenutačno navedeni u Prilogu III.

Uklanjanje primjera upotrebe visokorizičnih UI sustava iz Priloga III.

(22) U članku 7. stavku 3. UI akta utvrđeni su kriteriji za uklanjanje visokorizičnih UI sustava iz Priloga III. U tu svrhu Komisija mora dokazati da primjer upotrebe više ne predstavlja visok rizik od štete i da se njegovim uklanjanjem ne bi smanjila ukupna razina zaštite zdravlja i sigurnosti ili temeljnih prava u skladu s pravom Unije.

2.2. Metodologija za objektivno i participativno prikupljanje i analizu dokaza korištena u ovom izvješću i primijenjeni postupci

(23) U skladu s člankom 112. stavkom 11. UI akta, Ured za umjetnu inteligenciju dužan je razviti objektivnu i participativnu metodologiju za procjenu potrebe za preispitivanjem obuhvaćenim ovim izvješćem. Nadalje, u skladu s člankom 112. stavkom 8. i člankom 112. stavkom 9. UI akta, Komisija pri pripremi svojeg izvješća može zatražiti informacije od Europskog vijeća za umjetnu inteligenciju („Vijeće za umjetnu inteligenciju”), država članica i nacionalnih nadležnih tijela te pri provedbi preispitivanja i evaluacije mora uzeti u obzir stajališta i nalaze Vijeća za umjetnu inteligenciju, Europskog parlamenta, Vijeća i drugih relevantnih tijela ili izvora.

(24) U skladu s tim odredbama, Komisija je za pripremu ovog izvješća primijenila sljedeću metodologiju:

- **Suradnja s Vijećem za umjetnu inteligenciju i savjetovanje s državama članicama i nacionalnim nadležnim tijelima**

  Komisija je u postupku imenovanja surađivala s državama članicama i njihovim nacionalnim nadležnim tijelima, pri čemu je preko Vijeća za umjetnu inteligenciju uputio relevantna pitanja. U postupak je bilo uključeno nekoliko podskupina Vijeća za umjetnu inteligenciju.
- **Savjetovanje s dionicima**

  Provedeno je savjetovanje s više dionika kako bi se prikupile povratne informacije i stajališta širokog spektra dionika, uključujući predstavnike industrije, akademsku zajednicu, civilno društvo i širu javnost.
- **Empirijska istraživanja: analiza baza podataka o incidentima povezanima s umjetnom inteligencijom**

  Komisija je analizirala i relevantne baze podataka o incidentima povezanima s umjetnom inteligencijom kako bi razvila sveobuhvatan pristup utemeljen na empirijskim dokazima o šteti prouzročenoj UI sustavima.

(25) U odjeljcima u nastavku pobliže se opisuje metodologija za objektivno i participativno prikupljanje i analizu dokaza koja je primijenjena u ovom izvješću, odnosno pristupi primijenjeni za prikupljanje sveobuhvatnih informacija koje obuhvaćaju raznolike perspektive dionika, što doprinosi transparentnoj i utemeljenoj procjeni potkrijepljenoj dokazima.

3. Analiza prikupljenih informacija

3.1. Analiza informacija prikupljenih tijekom savjetovanja s državama članicama i Vijećem za umjetnu inteligenciju

(26) Ured za umjetnu inteligenciju savjetovao se s državama članicama u okviru relevantnih podskupina Vijeća za umjetnu inteligenciju[7] te ih pozvao da daju svoj doprinos izravno na sastancima ili u pisanom obliku.

3.1.1. Stajalište država članica o potrebi za preispitivanjem popisa zabranjenih praksi iz članka 5. UI akta

Opće stajalište

(27) Tijekom savjetovanja s relevantnom podskupinom Vijeća za umjetnu inteligenciju većina prisutnih država članica izjavila je da u ovoj fazi ne vidi potrebu za izmjenom popisa zabranjenih praksi u području umjetne inteligencije utvrđenog u članku 5. UI akta. Osim

[7] Konkretno, pitanja o potrebi za preispitivanjem popisa primjera upotrebe iz Priloga III. i popisa zabranjenih praksi u području umjetne inteligencije iz članka 5. UI akta dostavljena su državama članicama na četvrtom sastanku podskupine Vijeća za umjetnu inteligenciju za zabrane održanom 13. svibnja 2025., na trećem sastanku podskupine Vijeća iz Priloga III. za visokorizične UI sustave održanom 16. svibnja 2025., na trećem sastanku podskupine Vijeća iz Priloga III. za kazneni progon i sigurnost održanom 5. lipnja 2025. te na drugom sastanku podskupine Vijeća za umjetnu inteligenciju u financijskim uslugama održanom 13. svibnja 2025.

toga, devet država članica e-poštom je dostavilo pisane izjave i isto potvrdilo da ne postoji percipirana potreba za izmjenom tog popisa. Slične odgovore dostavila su i dva promatrača podskupine.

(28) Predstavnici država članica ispitanica u više su navrata napomenuli da evaluacija osobito štetnih praksi i praksi koje predstavljaju zlouporabu i koje su u suprotnosti s vrijednostima i temeljnim pravima EU-a tek počinje jer su se odredbe UI akta koje se odnose na definiciju UI sustava i zabranjenih praksi počele primjenjivati tek 2. veljače 2025., pravila o izvršavanju počet će se primjenjivati 2. kolovoza 2026., a mehanizmi izvršavanja još nisu u funkciji. Trenutačno nedostaje praktičnog iskustva i konkretnih primjera upotrebe na temelju kojih se može evaluirati djelotvornost zabrana iz UI akta jer se članak 5. Akta ne primjenjuje dugo. Stoga je procijenjeno da se smisleniji doprinos može pružiti nakon što relevantne odredbe budu dulje na snazi. Države članice zasad su napomenule da je dostupno malo konkretnih podataka ili analiza kojima bi se opravdala revizija.

(29) S obzirom na ta razmatranja, opće stajalište država članica bilo je da bi preispitivanje ili izmjena popisa zabranjenih praksi bili primjereniji u kasnijoj fazi, nakon što se prikupi dovoljno iskustva o provedbi.

Pitanja koja je potrebno dalje pratiti

(30) Jedna država članica predložila je da bi moglo biti relevantno procijeniti mogu li se na popis zabranjenih praksi u području umjetne inteligencije uvrstiti **UI sustavi namijenjeni razvoju ili distribuciji zlonamjernog softvera** koji bi mogli naštetiti kritičnoj infrastrukturi, ugroziti baze podataka ili stvoriti rizike za temeljna prava. Nakon analize tog prijedloga Komisija je smatrala da se čini da su rizici na koje bi se takva zabrana odnosila u dovoljnoj mjeri obuhvaćeni različitim zakonodavstvom EU-a[8], ali je to pitanje označila za daljnje praćenje i procjenu.

3.1.2. Stajališta država članica o potrebi za izmjenom primjera visokorizične upotrebe iz Priloga III. UI aktu

Opće stajalište

(31) Na nekoliko sastanaka podskupina Vijeća za umjetnu inteligenciju raspravljalo se o potrebi za izmjenom popisa primjera upotrebe iz Priloga III. UI aktu. Na tim su sastancima mnoge prisutne države članice izjavile da trenutačno ne smatraju da je potrebno izmijeniti Prilog III. Nadalje, sedam država članica e-poštom je dostavilo pisane izjave u kojima su potvrdile da u ovoj fazi ne vide potrebu za izmjenom Priloga III.

(32) Slično prethodno navedenim razmatranjima u vezi s mogućim izmjenama popisa zabranjenih praksi u području umjetne inteligencije iz članka 5. UI akta, države članice ispitanice u nekoliko su navrata napomenule da i dalje procjenjuju utjecaj zakonodavnog okvira na trenutačne primjere visokorizične upotrebe umjetne inteligencije navedene u

[8] Npr. zakonodavstvo EU-a iz područja kibernetičke sigurnosti (od nedavnih pravnih akata, vidjeti Akt EU-a o kibernetičkoj solidarnosti), Direktiva 2013/40/EU o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP.

Prilogu III. Pravila o visokorizičnim UI sustavima još se ne primjenjuju, a odgovarajuće smjernice Komisije o klasifikaciji visokorizičnih UI sustava još su u izradi. U tim okolnostima države članice općenito su smatrale da je preuranjeno mijenjati trenutačni popis primjera visokorizične upotrebe iz Priloga III. UI aktu.

Pitanja koja je potrebno dalje pratiti

(33) Dvije države članice izrazile su zabrinutost zbog određenih primjera upotrebe umjetne inteligencije[9].

(34) Jedan od razloga za zabrinutost bila je regulacija **(terapeutskih) UI *chatbotova* za samopomoć**[10] koji nisu obuhvaćeni Uredbom o medicinskim proizvodima[11]. Riječ je o digitalnim alatima koje pokreće umjetna inteligencija i koji su osmišljeni kako bi korisnicima pružili podršku u području mentalnog i emocionalnog zdravlja putem konverzacijskih sučelja. Iako su predstavljeni kao alati za dobrobit, a ne kao medicinski proizvodi, ipak utječu na odluke korisnika povezane s mentalnim zdravljem i mogu obrađivati osjetljive osobne podatke. Stoga postoji rizik da bi podrška i emocionalno savjetovanje koje takvi *chatbotovi* pružaju mogli negativno utjecati na mentalno zdravlje pojedinaca. Stoga je jedna država članica postavila pitanje ne bi li takvi sustavi trebali biti klasificirani kao visokorizični UI sustavi.

(35) Nakon analize tog pitanja Komisija smatra da *chatbotovi* za samopomoć koji odgovaraju definiciji medicinskog proizvoda podliježu strogim zahtjevima i kontrolama u skladu s Uredbom o medicinskim proizvodima. Nadalje, najštetniji UI *chatbotovi* za samopomoć potencijalno su obuhvaćeni zabranama iz članka 5. točaka (a) i (b) UI akta. Kad je riječ o klasifikaciji drugih UI *chatbotova* za samopomoć kao visokorizičnih, većina takvih UI sustava ne bi se mogla svrstati u neki od primjera upotrebe koji su trenutačno navedeni u Prilogu III., uz neke posebne iznimke koje su već obuhvaćene tim primjerima[12]. Osim toga, obveze otkrivanja utvrđene u članku 50. UI akta mogu barem donekle poslužiti za ublažavanje nekih rizika povezanih s UI *chatbotovima* za samopomoć, posebno onih povezanih s informiranim donošenjem odluka i mogućim psihološkim učinkom te interakcije na pojedince. Komisija će stoga procijeniti kako te odredbe u praksi ublažavaju prethodno navedene rizike prije nego što razmotri bilo kakve izmjene Priloga III. Komisija ipak uviđa da bi u ovoj fazi upotrebu i potencijalne rizike povezane s tom vrstom UI sustava trebalo pomno pratiti i prikupljati dodatne dokaze u narednim godinama, osobito nakon što se počnu primjenjivati odredbe UI akta o visokorizičnim UI sustavima.

(36) Zabrinutost izaziva i **personalizirano učenje koje se temelji na umjetnoj inteligenciji**. Trenutačna analiza na temelju kriterija navedenih u članku 7. UI akta navodi

[9] Kako je prethodno navedeno, Komisija će svoje smjernice o visokorizičnim UI sustavima objaviti tek 2026. Stoga se procjene konkretnih visokorizičnih UI sustava koje su utvrdile države članice, dionici ili baze podataka o incidentima povezanima s umjetnom inteligencijom temelje samo na tekstu UI akta. S obzirom na to da su trenutačno dostupne ograničene smjernice, konkretne procjene nisu uvijek bile moguće i ti su slučajevi označeni za daljnje praćenje.

[10] Sličnu zabrinutost izrazili su i drugi dionici (vidjeti odjeljak 3.2. u nastavku).

[11] Ako se *chatbot* stavlja na tržište kao pomoć za određene mentalne poremećaje ili za usmjeravanje korisnika kroz terapijske intervencije, vjerojatno je obuhvaćen područjem primjene Uredbe o medicinskim proizvodima jer se može smatrati softverom namijenjenim liječenju ili ublažavanju bolesti (članak 2. stavak 1. Uredbe o medicinskim proizvodima). 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.

[12] Na primjer, UI *chatbotovi* za samopomoć s funkcijama za prepoznavanje emocija. UI sustavi namijenjeni za prepoznavanje emocija klasificirani su kao visokorizični u skladu s Prilogom III. točkom 1. podtočkom (c).

Komisiju na zaključak da sustavi umjetne inteligencije sposobni za samostalno (neovisno) učenje u većini slučajeva ne predstavljaju jednakovrijedne ili veće rizike od onih koje predstavljaju UI sustavi navedeni u Prilogu III. UI aktu. Konkretno, postoje ograničeni empirijski dokazi o visokom riziku od štete povezanom s takvim sustavima i nisu utvrđeni incidenti koji uključuju te sustave. Sličan zaključak primjenjuje se na UI sustave koji se upotrebljavaju za razvoj personaliziranih materijala za učenje u kontekstu samostalnog (neovisnog) učenja. U predstojećim smjernicama Komisije o klasifikaciji visokorizičnih sustava dodatno će biti pojašnjeni drugi primjeri upotrebe personaliziranog učenja koje se temelji na umjetnoj inteligenciji.

(37) Naposljetku, jedna država članica predložila je proširenje Priloga III. UI aktu kako bi se obuhvatili primjeri upotrebe umjetne inteligencije za **odobrenja koja javna tijela izdaju** pojedincima za, primjerice, vozačku dozvolu, dozvolu za vatreno oružje i streljivo ili dozvolu za rukovanje kemijskim tvarima ili za rad s eksplozivima. U ovoj je fazi vrlo malo dokaza da takvi primjeri upotrebe opravdavaju klasifikaciju u visokorizičnu kategoriju na temelju kriterija iz članka 7. UI akta. Stoga Komisija smatra da te rizike treba dodatno pratiti.

3.2. Analiza doprinosa prikupljenih tijekom savjetovanja s dionicima

(38) Komisija je od 6. lipnja do 18. srpnja 2025. organizirala savjetovanje s više dionika[13] kako bi prikupila informacije o provedbi pravila UI akta o visokorizičnim UI sustavima. To je savjetovanje uključivalo i nekoliko pitanja o mogućoj potrebi za izmjenom popisa primjera visokorizične upotrebe iz Priloga III. UI aktu i popisa zabranjenih praksi u području umjetne inteligencije iz članka 5. UI akta.

(39) Zaprimljeno je ukupno 547 odgovora od raznih dionika, uključujući poduzeća, organizacije civilnog društva, akademsku zajednicu, javne institucije i pojedince koji djeluju kao privatne osobe[14].

3.2.1. Stajališta dionika o potrebi za preispitivanjem popisa zabrana iz članka 5. UI akta

(40) Iako je velik broj dionika smatrao da je postojeći popis dostatan[15], neki su predložili uvrštavanje dodatnih zabrana[16]. Većina dionika ispitanika nije se zalagala za ukidanje bilo koje postojeće zabrane.

---

[13] Komisija pokreće javno savjetovanje o visokorizičnim UI sustavima | Europski portal e-pravosuđe.

[14] Ukupno 409 ispitanika navelo je da predstavljaju organizacije. Među njima su najveću skupinu činili ispitanici koji su predstavljali poduzeća (150 odgovora), zatim udruženja (93 odgovora) te ispitanici koji su odabrali opciju „druga organizacija" (81 odgovor). Na organizacije ili udruge civilnog društva odnosilo se 56 odgovora, a manji dio organizacija činili su istraživački instituti (11 odgovora), sveučilišta (7 odgovora), skupine za strateško promišljanje (6 odgovora) i organizacije potrošača (5 odgovora). Ukupno 138 ispitanika navelo je da sudjeluju kao pojedinci. Među njima je najviše bilo onih koji su se izjasnili kao drugi neovisni stručnjaci ili članovi organizacija s relevantnim stručnim znanjem (35), dobavljači UI sustava (34) i pripadnici akademske zajednice (28), dok ih je 14 odabralo kategoriju „drugo", a 13 ih je navelo da su subjekti koji uvode UI sustave. Neki drugi ispitanici koji su izjavili da sudjeluju kao privatne osobe naveli su poveznicu s organizacijom civilnog društva (7), drugim operaterima (3), poslovnim udruženjem (2) ili nadzornim tijelima (2).

[15] Smatralo se da i ispitanici koji su to izričito naveli u svojim odgovorima i oni koji nisu komentirali relevantno pitanje smatraju da je trenutačni popis zabrana dostatan.

[16] Nešto više od 10 % ispitanika.

(41) Komisija je evaluirala prijedloge dionika za uvrštavanje dodatnih zabrana primjenom metodologije i kriterija navedenih u odjeljku 2.1.1. Konkretno, Komisija je na temelju zaprimljenih prijedloga nastojala utvrditi one prakse koje se mogu smatrati posebno štetnima i koje predstavljaju zlouporabu te su u suprotnosti s vrijednostima i temeljnim pravima EU-a, a nisu u dovoljnoj mjeri obuhvaćene postojećim zakonodavstvom EU-a. Na temelju tog pristupa procijenilo se trebaju li predloženi dodaci biti uvršteni na popis zabranjenih praksi u području umjetne inteligencije ili ih se može uzeti u obzir u drugim regulatornim mehanizmima u okviru UI akta ili eventualno drugog zakonodavstva EU-a.

(42) Procijenjeno je da je znatan broj prijedloga u dovoljnoj mjeri obuhvaćen postojećim odredbama UI akta, i to zabranama iz članka 5. UI akta, klasifikacijom određenih UI sustava kao visokorizičnih na temelju Priloga III. ili Priloga I. UI aktu ili zahtjevima u pogledu transparentnosti iz članka 50. UI akta. Čini se da neki prijedlozi ne ispunjavaju prag za zabranu na temelju UI akta kad ih se procjenjuje uzimajući u obzir trenutačnu fazu razvoja i primjene umjetne inteligencije te prijavljene incidente povezane s umjetnom inteligencijom[17].

(43) Dionici su u više navrata izrazili zabrinutost u vezi sa sljedećim pitanjima koja su označena za daljnje praćenje i evaluaciju prakse:

- u području biometrije, brojni prijedlozi odnosili su se na proširenje zabrane upotrebe **tehnologija za prepoznavanje emocija** iz članka 5. stavka 1. točke (f) UI akta. Takva je upotreba zabranjena na radnom mjestu i u obrazovnim ustanovama[18], a u svim drugim područjima klasificirana je u kategoriju visokorizičnih UI sustava u skladu s točkom 1. Priloga III. UI aktu. Nadalje, u skladu člankom 50. stavkom 3. UI akta subjekti koji uvode sustave za prepoznavanje emocija moraju o radu sustava obavijestiti pojedince koji su im izloženi. Međutim, nekoliko ispitanika izrazilo je zabrinutost zbog njihova uvođenja u osjetljivim kontekstima, kao što su migracije, te je predložilo da se njihova upotreba u tim konkretnim područjima izričito zabrani umjesto da se na njih primjenjuju regulatorni zahtjevi koji se odnose na visokorizične sustave. Zbog nedostatka empirijskih dokaza da klasifikacija takvih sustava kao visokorizičnih nije dovoljna za osiguravanje zaštite temeljnih prava, Komisija ne vidi hitnu potrebu za izmjenom članka 5. UI akta u tom smislu. Međutim, to je područje označeno za daljnje razmatranje.

- Nekoliko dionika postavilo je pitanje o klasifikaciji **UI sustava koji omogućuju tamne obrasce i dizajn koji stvara ovisnost**. Komisija trenutačno procjenjuje da su najštetniji slučajevi takvih praksi već obuhvaćeni postojećim zabranama, točnije onima navedenima u članku 5. točkama (a) i (b) UI akta. Nadalje, te prakse mogu biti obuhvaćene drugim zakonodavstvom EU-a, kao što su Direktiva o nepoštenoj poslovnoj praksi[19] i Akt o digitalnim uslugama[20], bez obzira na to jesu li omogućene

[17] Kao što su, na primjer, prijedlozi za zabranu UI sustava koji se koriste za upravljanje migracijama; kloniranje glasa u UI aplikacijama usmjerenima na potrošače; ili generiranje izmišljenih osoba umjetnom inteligencijom koje se koristi za političke poruke.

[18] Osim ako se UI sustav namjerava staviti u upotrebu ili na tržište iz medicinskih ili sigurnosnih razloga.

[19] Direktiva 2005/29/EZ Europskog parlamenta i Vijeća od 11. svibnja 2005. o nepoštenoj poslovnoj praksi poslovnog subjekta u odnosu prema potrošaču na unutarnjem tržištu i o izmjeni Direktive Vijeća 84/450/EEZ, direktiva 97/7/EZ, 98/27/EZ i 2002/65/EZ Europskog parlamenta i Vijeća, kao i Uredbe (EZ) br. 2006/2004 Europskog parlamenta i Vijeća („Direktiva o nepoštenoj poslovnoj praksi"). SL L 149, 11.6.2005., str. 22.

[20] Uredba (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama). SL L 277, 27.10.2022., str. 1.

umjetnom inteligencijom. Međutim, takve su prakse i dalje bitno područje koje izaziva zabrinutost. Smatra se važnim pomno pratiti njihov razvoj kako bi se procijenilo pruža li postojeće zakonodavstvo EU-a i dalje odgovarajuću zaštitu, osobito ako UI sustavi omogućuju tamne obrasce i dizajn koji stvara ovisnost.

- Nekoliko dionika skrenulo je pozornost na UI sustave koji **olakšavaju prijevare** i **generiraju nage slike te druge zlonamjerne i ponižavajuće uvjerljive krivotvorene sadržaje** (eng. *deepfake*). Te štetne prakse utvrđene su i u analizi incidenata te su dodatno razmotrene u odjeljku 3.3.3.

3.2.2. Stajališta dionika o potrebi za izmjenom primjera upotrebe iz Priloga III. UI aktu

(44) Premda je velik broj dionika smatrao da je postojeći popis visokorizičnih slučajeva upotrebe iz Priloga III. UI aktu adekvatan[21], neki su predložili dodavanje novih primjera upotrebe u kategorije područja, proširenje postojećih primjera ili su postavili pitanje bi li u prilog trebalo dodati nove kategorije područja[22]. Većina dionika nije podržala uklanjanje nijednog postojećeg primjera upotrebe iz Priloga III.

(45) Komisija je procijenila da je znatan broj prijedloga u dovoljnoj mjeri obuhvaćen postojećim odredbama UI akta[23]. Evaluirani su preostali prijedlozi za uvrštavanje dodatnih primjera upotrebe i kategorija područja, pri čemu su se uzeli u obzir kriteriji iz članka 7. UI akta (vidjeti odjeljak 2.1.2.). Preispitano je nekoliko predloženih primjera upotrebe, ali se nije smatralo da je rizik od štete koji predstavljaju jednakovrijedan ili veći od rizika koji su već navedeni u Prilogu III. UI aktu[24]. Za neka pitanja koja su istaknuli dionici procijenjeno je da su vjerojatno već obuhvaćena popisom primjera visokorizične upotrebe iz Priloga III. UI aktu te je napomenuto da će ih se dodatno pojasniti u smjernicama o klasifikaciji visokorizičnih UI sustava koje Komisija trenutačno sastavlja[25].

(46) Komisija je za sljedeća pitanja, u vezi s kojima su dionici opetovano izrazili zabrinutost, utvrdila da ih je potrebno kontinuirano pratiti i procijeniti s obzirom na razvoj praksi:

- Znatan broj prijedloga odnosio se na **točku 5. Priloga III. UI aktu**. Kad je riječ o točki 5. podtočki (a), nekoliko dionika dovelo je u pitanje nepostojanje izričitog upućivanja na UI sustave koji se upotrebljavaju u javnoj upravi za upravljanje pristupom naknadama socijalne skrbi i socijalnim stanovima. Kad je riječ o točki 5. podtočki (b), dionici su napomenuli da UI sustavi koji se upotrebljavaju za provjeru najmoprimaca i utvrđivanje prihvatljivosti u privatnim uslugama (npr. telekomunikacije, komunalne usluge) nisu jasno obuhvaćeni. Kad je riječ o točki 5.

[21] Smatralo se da i ispitanici koji su to izričito naveli u svojim odgovorima i oni koji nisu komentirali relevantno pitanje smatraju da je trenutačni popis primjera visokorizične upotrebe umjetne inteligencije u Prilogu III. adekvatan.
[22] Oko 20 % ispitanika.
[23] Kao što su, na primjer, prijedlozi za uključivanje posebnih biometrijskih sustava kao visokorizičnih (već obuhvaćeni točkom 1. Priloga III.).
[24] Na primjer, UI sustavi osmišljeni kako bi pružatelji internetskih usluga osigurali odgovarajuću vidljivost audiovizualnih medijskih usluga od javnog interesa; određeni UI sustavi koji se upotrebljavaju u uzgoju životinja.
[25] Na primjer, zabrinutost koju su dionici izrazili zbog određenih UI sustava koji se upotrebljavaju prilikom zapošljavanja i za prepoznavanje emocija.

podtočki (c), izražena je zabrinutost da je trenutačni visokorizični primjer upotrebe ograničen na životno i zdravstveno osiguranje, a ne navode se druga osnovna osiguranja (npr. motorna vozila, profesionalna odgovornost, osiguranje nekretnina, invalidsko osiguranje). Izneseni su i prijedlozi za proširenje točke 5. podtočke (d) kako bi se uključili UI sustavi koji imaju utjecaj na odluke o odgovoru na hitne situacije koje utječu na sigurnost i prava (npr. prisilna evakuacija, ograničenja kretanja). Mnogi su prijedlozi uzeti u obzir radi dodatnog pojašnjenja u predstojećim smjernicama Komisije o klasifikaciji visokorizičnih sustava, a Ured za umjetnu inteligenciju pomno će pratiti uvođenje UI sustava u području obuhvaćenom točkom 5. Priloga III. UI aktu, posebno u situacijama za koje u tom prilogu ne postoji relevantan primjer visokorizične upotrebe koji se odnosi na konkretne UI sustave. Posebna pozornost posvetit će se prikupljanju empirijskih podataka o stvarnim štetama i utvrđivanju svih regulatornih nedostataka koji bi mogli nastati, a koji bi mogli opravdati izmjenu ili dopunu popisa primjera visokorizične upotrebe iz točke 5. Priloga III. ili općenito kategorija područja.

- U savjetovanju s dionicima ponavljalo se pitanje u vezi s kojim je jedna država članica izrazila zabrinutost (vidjeti odjeljak 3.1.), a odnosilo se na **UI suradnike i UI *chatbotove* za mentalnu podršku**. Dionici su te UI sustave naveli u kontekstu moguće potrebe za izmjenom zabranjenih praksi u području umjetne inteligencije i u kontekstu primjera upotrebe iz Priloga III. Kako je prethodno navedeno, ako takvi sustavi imaju subliminalni, manipulativni ili obmanjujući utjecaj ili iskorištavaju ranjivosti na štetan način, mogu biti obuhvaćeni zabranama iz članka 5. točaka (a) i (b) UI akta. Ako su dizajnirani s elementima za prepoznavanje emocija, mogu se klasificirati kao visokorizični u skladu s točkom 1. podtočkom (c) Priloga III. UI aktu. Obveze u pogledu transparentnosti primjenjuju se i kako bi korisnici bili svjesni da su u interakciji s UI okvirom za razgovor ili da su izloženi sustavima za prepoznavanje emocija ili biometrijsku kategorizaciju. Dodatne zaštitne mjere predviđene su Aktom o digitalnim uslugama[26] i pravom EU-a o zaštiti podataka, ako je primjenjivo[27]. Međutim, s obzirom na sve češću upotrebu UI suradnika i UI *chatbotova* za mentalnu podršku, Komisija smatra da je važno pomno pratiti njihov razvoj u narednim godinama kako bi se prikupili dodatni dokazi i procijenilo je li postojeći zakonodavni okvir i dalje adekvatan za uklanjanje rizika koji oni mogu predstavljati.

[26] Aktom o digitalnim uslugama zabranjuje se manipulativni dizajn sučelja (tamni obrasci), a pružatelje vrlo velikih internetskih platformi i vrlo velikih internetskih tražilica obvezuje se da utvrde, procijene i analiziraju sve sistemske rizike koji proizlaze iz dizajna ili funkcioniranja njihovih usluga i povezanih sustava, uključujući algoritamske sustave (članak 34. Akta o digitalnim uslugama). Pružatelji usluga dužni su uspostaviti i razumne, razmjerne i djelotvorne mjere za smanjenje rizika, uključujući testiranje i prilagodbu svojih algoritamskih sustava (članak 35. Akta o digitalnim uslugama). Akt o digitalnim uslugama propisuje i da pružatelji internetskih platformi dostupnih maloljetnicima moraju uspostaviti odgovarajuće i razmjerne mjere kako bi osigurali visoku razinu privatnosti, sigurnosti i zaštite maloljetnika na svojoj usluzi (članak 28. stavak 1. Akta o digitalnim uslugama). Uredba (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama). SL L 277, 27.10.2022., str. 1.

[27] Kao što su načela obrade podataka i prava ispitanika utvrđena Općom uredbom o zaštiti podataka (OUZP) koja bi se primjenjivala u vezi s UI sustavom, npr. zato što se osobni podaci upotrebljavaju za razvoj UI sustava ili predstavljaju ulazne ili izlazne podatke tijekom uvođenja. 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.

- Neki su dionici predložili da se **UI sustavi koji se upotrebljavaju za naplatu duga** klasificiraju kao visokorizični, napominjući da ih pružatelji usluga u području energije, telekomunikacija i financijskih usluga sve više upotrebljavaju. Takvi UI sustavi mogli bi biti obuhvaćeni kategorijom područja iz točke 5. ili 8. Priloga III. UI aktu. Komisija će dodatno pratiti te sustave kako bi utvrdila intenzitet njihove primjene i moguću štetu, posebno u odnosu na ranjive potrošače.

- Nekoliko dionika predložilo je proširenje područja primjene točke 2. Priloga III. UI aktu, koja se odnosi na UI sustave koji se koriste u području **kritične infrastrukture**. Smatrali su da to područje ne bi trebalo obuhvaćati samo UI sustave koji funkcioniraju kao sigurnosne komponente, već i širu lepezu sustava koji su ključni za pouzdanost i kontinuitet infrastrukture. S obzirom na te prijedloge, potrebno je daljnje praćenje UI sustava u tom području kako bi se procijenili intenzitet uvođenja i štete koje takvi sustavi mogu uzrokovati u praksi.

3.3. Empirijska istraživanja: analiza baza podataka o incidentima povezanima s umjetnom inteligencijom i drugih izvora

(47) Za potrebe ovog izvješća pregledane su i analizirane i informacije u relevantnim bazama podataka o incidentima povezanima s umjetnom inteligencijom. To uredsko istraživanje provedeno je kako bi se utvrdile opasne prakse i raniji incidenti koje su izazvali UI sustavi i koji bi mogli pružiti empirijske dokaze o rizicima za zdravlje, sigurnost i temeljna prava koji su nastupili te kako bi se time doprinijelo procjeni preispitivanja. Empirijsko istraživanje iz sljedećeg odjeljka, premda predstavlja dodatni izvor dostupnih podataka o šteti i incidentima prouzročenima UI sustavima koji se mogu koristiti za mapiranje, inherentno je ograničeno jer analizirane baze podataka o incidentima ne sadržavaju cjelovite i provjerene informacije o incidentima povezanima s umjetnom inteligencijom. Osim toga, mnogi su incidenti globalni, odnosno nisu ograničeni na Europu, pa nisu uvijek dostupne detaljne informacije za adekvatnu kategorizaciju incidenata prema UI aktu.

3.3.1. Baze podataka i vremenski okvir

(48) Glavna baza podataka na koju se oslanjalo to uredsko istraživanje bio je alat za praćenje incidenata i opasnosti povezanih s umjetnom inteligencijom[28] Organizacije za gospodarsku suradnju i razvoj (OECD). Ta je baza podataka besplatan projekt otvorenog koda namijenjen indeksiranju povijesti štetnih ili gotovo štetnih događaja koji su se dogodili u

[28] Dostupno na https://oecd.ai/en/incidents?search_terms=%5B%5D&and_condition=false&from_date=2014-01-01&to_date=2025-05-27&properties_config=%7B%22principles%22:%5B%5D,%22industries%22:%5B%5D,%22harm_types%22:%5B%5D,%22harm_levels%22:%5B%5D,%22harmed_entities%22:%5B%5D%7D&only_threats=false&order_by=date&num_results=20.

stvarnom svijetu zbog primjene UI sustava. Ta baza podataka temelji se na umjetnoj inteligenciji i prikuplja informacije o incidentima povezanima s umjetnom inteligencijom iz javnih izvora (uglavnom o incidentima povezanima s umjetnom inteligencijom o kojima su izvještavali mediji). Još jedna baza podataka koju je Komisija pregledala bio je repozitorij rizika u području umjetne inteligencije[29] Tehnološkog instituta u Massachusettsu (Massachusetts Institute of Technology, MIT)[30]. Ta je baza podataka uglavnom analizirana radi izrade metodologije analize incidenata.

(49) S obzirom na to da se u bazama podataka o incidentima objavljuju samo kratki sažeci prijavljenih događaja, analize koje se oslanjaju na te izvore bile su u određenoj mjeri ograničene. Sažeti opisi ne omogućuju uvijek preciznu evaluaciju obilježja incidenata ni točnu kategorizaciju u skladu s metodološkim okvirom primijenjenim u ovom izvješću, kako je navedeno u odjeljku 2.1. Zbog tih ograničenja u ovom se izvješću upotrebljavaju općeniti izrazi za kvantificiranje (kao što su „znatan dio” ili „mali dio”) umjesto navođenja točnih udjela incidenata.

(50) Kako bi bilo dovoljno vremena za analizu incidenata, obuhvaćeni vremenski okvir bio je ograničen na incidente prijavljene od 1. siječnja 2024. (nakon dovršetka pregovora o UI aktu) do 31. svibnja 2025. U tom je razdoblju u alatu OECD-a za praćenje incidenata i opasnosti povezanih s umjetnom inteligencijom prijavljen ukupno 3 791 incident.

3.3.2. Kategorizacija prijavljenih incidenata

(51) Prvi korak analize bila je kategorizacija svakog prijavljenog incidenta (3 791) u šest kategorija. Te su kategorije:

1. incidenti koji nisu obuhvaćeni područjem primjene UI akta;
2. incidenti koji su vjerojatno obuhvaćeni Prilogom I. UI aktu;
3. incidenti koji su vjerojatno obuhvaćeni člankom 50. UI akta;
4. incidenti koji predstavljaju hipotetske rizike, ali do trenutka prijavljivanja nisu prouzročili nikakvu štetu;
5. incidenti koji su (ili bi mogli biti) potencijalno obuhvaćeni člankom 5. UI akta; i
6. incidenti koji su (ili bi mogli biti) potencijalno obuhvaćeni Prilogom III. UI aktu.

(52) Premda su kategorije od 1. do 4. prikupljene u svrhu boljeg razumijevanja općeg konteksta incidenata povezanih s umjetnom inteligencijom, dodatno su analizirani samo incidenti obuhvaćeni kategorijama 5. i 6. u skladu s metodologijom primijenjenom u ovom izvješću i navedenim kriterijima (odjeljak 2.1.).

[29] Dostupno na https://airisk.mit.edu/.

[30] Repozitorij se sastoji od tri dijela: (i) baze podataka o rizicima u području umjetne inteligencije, (ii) taksonomije uzroka rizika u području umjetne inteligencije (u kojoj se klasificira kako, kada i zašto nastaju rizici u području umjetne inteligencije) i taksonomije područja rizika u području umjetne inteligencije (razvrstavanje rizika u području umjetne inteligencije u sedam područja (npr. „pogrešne informacije”) i 24 potpodručja (npr. „lažne ili obmanjujuće informacije”)).

(53) Analiza je pokazala da gotovo polovina svih prijavljenih incidenata u relevantnom razdoblju nije obuhvaćena područjem primjene UI akta ili je u dovoljnoj mjeri obuhvaćena drugim instrumentima EU-a[31]. Osim toga, otprilike 10 % prijavljenih incidenata vjerojatno bi bilo obuhvaćeno Prilogom I. UI aktu[32] i stoga se očekuje da će biti otklonjeni nakon što se ta pravila UI akta počnu primjenjivati. Čini se da je dio prijavljenih incidenata obuhvaćen člankom 50. UI akta[33] i stoga se isto može očekivati da će biti otklonjeni kad se taj dio UI akta počne primjenjivati. Naposljetku, neki od prijavljenih incidenata bili su hipotetski incidenti i stoga su isključeni iz daljnje analize, koja je bila ograničena na stvarnu štetu koja je nastala ili je bilo razumno očekivati da će nastati zbog incidenta.

(54) Komisija je utvrdila da je za detaljniju analizu relevantno oko 30 % prijavljenih incidenata. Otprilike dvije trećine tih incidenata bilo je obuhvaćeno područjem primjene članka 5. UI akta ili se smatralo da su dovoljno relevantni da je opravdano procijeniti ispunjavaju li kriterije za uvrštavanje na popis zabranjenih praksi u području umjetne inteligencije (odjeljak 2.1.1.). Preostala trećina incidenata određenih za detaljniju analizu vjerojatno bi bila obuhvaćena visokorizičnim kategorijama područja navedenima u Prilogu III. UI aktu[34]. Međutim, trebalo je provjeriti jesu li ti incidenti obuhvaćeni primjerima visokorizične upotrebe koji su trenutačno navedeni u Prilogu III. ili, ako nisu, ispunjavaju li kriterije za uvrštavanje u taj prilog (kriteriji navedeni u odjeljku 2.1.2.).

3.3.3. Procjena incidenata određenih za daljnju procjenu

(55) Drugi korak analize uključivao je procjenu je li 30 % prijavljenih incidenata za koje je utvrđeno da su relevantni za detaljniju analizu obuhvaćeno zabranama iz članka 5. ili primjerima upotrebe iz Priloga III. UI aktu. Ako nisu bili, sljedećom procjenom nastojalo se utvrditi postoji li potreba za izmjenom tih odredaba dodavanjem ili uklanjanjem relevantnih primjera upotrebe.

Incidenti potencijalno obuhvaćeni zabranjenim praksama u području umjetne inteligencije navedenima u članku 5. UI akta

(56) Kad je riječ o incidentima koji bi mogli biti obuhvaćeni zabranama iz članka 5. UI akta, čini se da je dio procijenjenih incidenata već obuhvaćen tom odredbom[35]. Neki od

[31] Ti su se incidenti općenito odnosili na pitanja obuhvaćena drugim relevantnim zakonodavstvom EU-a, kao što su povrede privatnosti podataka, koja su uređena OUZP-om. Osim toga, mnogi od tih incidenata odnosili su se na sporove o autorskom pravu, koji su obuhvaćeni instrumentima kao što je zakonodavstvo EU-a o autorskom pravu. Nadalje, mnogi incidenti spadaju u područja koja su u nadležnosti država članica, kao što je upotreba umjetne inteligencije u vojne svrhe.

[32] Takvi incidenti prvenstveno su se odnosili na štetu nastalu zbog primjene umjetne inteligencije u medicinskim proizvodima ili autonomnim vozilima.

[33] Ti se incidenti odnose na uvjerljiv krivotvoreni sadržaj bez odgovarajućih vodenih žigova ili drugih mjera transparentnosti.

[34] Ti su se incidenti najčešće odnosili na upotrebu umjetne inteligencije u biometrijskoj identifikaciji u kaznenom progonu, upravljanju nadzorom državne granice, osnovnim uslugama, obrazovnim i strukovnim ustanovama te u pravosuđu i demokratskim procesima.

[35] Takvi incidenti, koji su potencijalno bili obuhvaćeni člankom 5. UI akta, pokrivali su niz tema, kao što su biometrijska identifikacija u stvarnom vremenu ili prepoznavanje emocija na radnom mjestu.

incidenata nisu se mogli smatrati obuhvaćenima zabranama iz članka 5. UI akta niti isključenima iz njih zbog nedostatka informacija za konkretnu procjenu.

(57) Međutim, Komisija je utvrdila da je znatan broj incidenata potencijalno povezan sa zabranjenim praksama iz članka 5. UI akta ili da predstavljaju slične prakse s posebno štetnim učincima i učincima zlouporabe koje nisu jasno obuhvaćene tom odredbom. Ti su incidenti procijenjeni u skladu s kriterijima iz odjeljka 2.1.1. Na temelju te analize Komisija je utvrdila sljedeća područja:

- UI sustavi namijenjeni ili sposobni za generiranje **seksualno eksplicitnog uvjerljivog krivotvorenog sadržaja nastalog bez pristanka** koji prikazuje stvarne osobe, uključujući maloljetnike. Komisija je analizirala bi li postojeće zabrane UI sustava koji primjenjuju namjerno manipulativne ili obmanjujuće tehnike (članak 5. stavak 1. točka (a) UI akta) ili iskorištavaju slabosti zbog dobi, invaliditeta ili posebne socioekonomske situacije (članak 5. stavak 1. točka (b)) koja uzrokuje znatnu štetu mogle obuhvaćati UI sustave koji proizvode materijal koji sadržava seksualno zlostavljanje djece i seksualno eksplicitne slike koje se dijele bez pristanka. Komisija zaključuje da te prakse nisu obuhvaćene člankom 5. stavkom 1. točkom (a) ni člankom 5. stavkom 1. točkom (b) UI akta jer se njima ne manipulira djecom i žrtvama kako bi ih se uključilo u štetno ponašanje.

- UI sustavi namijenjeni za **olakšavanje prijevara i financijskih prijevara** mogli bi potencijalno biti obuhvaćeni člankom 5. stavkom 1. točkama (a) i (b) UI akta ako su ispunjeni uvjeti iz tih odredaba, uključujući prag znatne financijske štete. To nužno zahtijeva i vjerodostojnu uzročno-posljedičnu vezu između financijske štete koja je nastala ili je razumno očekivati da će nastati i upotrebe UI sustava (npr. uvjerljiv krivotvoreni sadržaj koji oponaša člana obitelji). Komisija smatra da je važno evaluirati kako se razvija praksa država članica u pogledu tumačenja zahtjeva o znatnoj financijskoj šteti i kako će to utjecati na obuhvaćanje takvih štetnih i prijevarnih praksi u području umjetne inteligencije zabranama iz članka 5. UI akta.

Incidenti povezani s primjerima visokorizične upotrebe iz Priloga III.

(58) Analiza incidenata koji spadaju u visokorizične kategorije područja iz Priloga III. UI aktu pokazala je da je velik dio već vjerojatno obuhvaćen konkretnim primjerima upotrebe iz tog priloga[36]. Osim toga, ocijenjeno je da neki prijavljeni incidenti ne predstavljaju razinu rizika od štete jednakovrijednu onoj koja je povezana s primjerima upotrebe koji su već

[36] Incidenti u području biometrije (točka 1. Priloga III.) često su se odnosili na UI sustave korištene u nadzornim kamerama za daljinsko prepoznavanje lica radi identifikacije osumnjičenika. U području zapošljavanja utvrđeni incidenti bili su povezani s UI sustavima koji se upotrebljavaju za optimizaciju postupaka zapošljavanja i otpuštanja, kao što su pregledavanje životopisa ili nadzor zaposlenika na platformama koje se upotrebljavaju na radnom mjestu. Kad je riječ o pristupu osnovnim uslugama i njihovu korištenju, prijavljeni incidenti često su se odnosili na upotrebu algoritma koji se temelji na umjetnoj inteligenciji za označavanje osoba koje primaju naknadu za troškove stanovanja kao mogućih počinitelja prijevare, što dovodi do nepotrebnih istraga i kršenja prava. U području kaznenog progona, relevantni incidenti uključuju upotrebu umjetne inteligencije za procjenu rizika s kojima se suočavaju žrtve obiteljskog nasilja. Kad je riječ o upravljanju nadzorom državne granice, relevantni incidenti odnosili su se na praćenje i identifikaciju lica migranata putem kamera.

navedeni u Prilogu III. UI aktu[37]. Manji udio incidenata nije se mogao sa sigurnošću kategorizirati zbog nedostatnih informacija.

(59) Utvrđeno je da je znatan broj incidenata obuhvaćen kategorijama područja iz Priloga III. UI aktu; međutim, oni nisu bili jasno obuhvaćeni konkretnim primjerima upotrebe koji su u njima trenutačno navedeni. Ti su incidenti procijenjeni na temelju kriterija iz odjeljka 2.1.2. Analizom su utvrđena sljedeća područja označena za daljnje praćenje i prikupljanje podataka:

- Velik broj incidenata uključivao je **političke kampanje dezinformiranja**, koje su tematski obuhvaćene područjem pravosuđa i demokratskih procesa navedenih u točki 8. Priloga III., ali nisu jasno navedene u primjerima upotrebe iz te točke. Te kampanje dezinformiranja uglavnom su se odnosile na uvjerljivo krivotvorene videozapise i slike, a rizici povezani s tim već su u određenoj mjeri obuhvaćeni člankom 50. UI akta. Nadalje, dio takvih UI sustava može biti obuhvaćen zabranama iz članka 5. stavka 1. točaka (a) ili (b) UI akta, pod uvjetom da su ispunjeni svi uvjeti navedeni u tom članku. Osim toga, Akt o digitalnim uslugama i Uredba o transparentnosti i ciljanju u političkom oglašavanju[38] bave se nekim od pitanja povezanih s političkim dezinformacijama. U nedavno donesenoj Komunikaciji o europskom štitu za zaštitu demokracije[39] predviđene su dodatne mjere i inicijative. Komisija će u predstojećim smjernicama o klasifikaciji visokorizičnih UI sustava dodatno procijeniti i razjasniti može li se dio takvih praksi u području umjetne inteligencije klasificirati kao UI sustavi namijenjeni za utjecanje na ishod izbora ili referenduma ili na ponašanje pojedinaca prilikom glasovanja na izborima ili referendumima.

Zaključak

(60) Ovo izvješće priprema Komisija i upućuje ga Europskom parlamentu i Vijeću kako bi ispunila svoje obveze utvrđene u članku 112. stavku 1. UI akta. Nalazi navedeni u ovom izvješću podnose se na razmatranje tim institucijama.

(61) Nakon procjene provedene primjenom objektivne i participativne metodologije za preispitivanje propisano člankom 112. stavkom 1. UI akta Komisija primjećuje i dodatno

[37] Nekoliko incidenata uključivalo je upotrebu kamera umjetne inteligencije za otkrivanje prometnih prekršaja ili praćenje gustoće mnoštva i postizanje sigurnosti na javnim događanjima. Takve primjene umjetne inteligencije odnose se na kazneni progon, međutim, čini se da ne predstavljaju rizik od štete koji je jednakovrijedan ili veći od rizika od štete ili nepovoljnog utjecaja koji predstavljaju drugi visokorizični UI sustavi koji su već navedeni u točki 6. Priloga III. To je uglavnom zbog toga što se obično odnose na prekršaje čije su posljedice manje nametljive od onih povezanih s kaznenim djelima ili se upotrebljavaju za postizanje sigurnosti bez izravnog učinka na temeljna prava. U skladu s tim, za takve primjere upotrebe umjetne inteligencije trenutačno nije potrebna izmjena Priloga III.

[38] Uredba (EU) 2024/900 Europskog parlamenta i Vijeća od 13. ožujka 2024. o transparentnosti i ciljanju u političkom oglašavanju. SL L, 2024/900, 20.3.2024.

[39] Zajednička komunikacija Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, Europski štit za zaštitu demokracije: za jača i otpornija demokratska društva. Bruxelles, 12.11.2025. JOIN(2025) 791 final.

analizira moguću regulatornu prazninu u pogledu UI sustava koji generiraju sadržaj koji sadržava seksualno zlostavljanje djece i intimni sadržaj koji se dijeli bez pristanka, koji nisu zabranjeni člankom 5. UI akta. Budući da su se odredbe UI akta koje se odnose na zabranjene prakse u području umjetne inteligencije počele primjenjivati 2. veljače 2025., a pravila o izvršavanju još se ne primjenjuju, procjena drugih posebno štetnih praksi i praksi zlouporabe u području umjetne inteligencije koje su u suprotnosti s vrijednostima i temeljnim pravima EU-a još je u ranoj fazi te nedostaje praktično iskustvo sa zabranama. Opsežnija evaluacija primjene članka 5. UI akta bit će moguća tek nakon što se te zabrane budu primjenjivale najmanje godinu dana i nakon što zajednički problemi ili regulatorni nedostaci postanu očiti. Slično tome, evaluacija funkcioniranja pravila o visokorizičnim UI sustavima i utvrđivanje mogućih nedostataka u upotrebi takvih sustava koji predstavljaju visok rizik od štete za zdravlje i sigurnost ili temeljna prava bit će lakši nakon što Komisija objavi smjernice o klasifikaciji visokorizičnih UI sustava i nakon što se stekne praktično iskustvo. Očekuje se i da će regulatorna izolirana okruženja uspostavljena u skladu s UI aktom služiti kao mehanizam za regulatorno učenje i prikupljanje dokaza koji će pomoći u utvrđivanju mogućih regulatornih nedostataka i problema u tumačenju. Na temelju prikupljenih dokaza i procjene iz ovog izvješća Komisija je ipak označila određene UI sustave za praćenje i daljnju analizu u budućim preispitivanjima.

(62) Tijela za nadzor tržišta koja nadziru primjenu UI akta potiču se da u narednim godinama razmotre, na temelju svojeg praktičnog iskustva u nadzoru i izvršavanju, uzimaju li zabrane iz članka 5. UI akta adekvatno u obzir zlonamjerne i konkretne primjene s velikim potencijalom za zlouporabu. Slično tome, nakon početka primjene i izvršavanja pravila o visokorizičnim UI sustavima, posebnu pozornost trebalo bi posvetiti UI sustavima koji bi se mogli razvrstati u jedno od područja navedenih u Prilogu III., ali nisu izričito navedeni na trenutačnom popisu primjera visokorizične upotrebe. Time će se osigurati informacije utemeljene na dokazima za buduća izvješća Komisije donesena na temelju članka 112. stavka 1. UI akta i pomoći Komisiji da procijeni je li područje primjene članka 5. UI akta i njegova Priloga III. i dalje adekvatno nakon proteka vremena, čime će se otvoriti put za dobro informirano i objektivno preispitivanje utemeljeno na dokazima i moguću reviziju relevantnih odredaba UI akta.

(63) U skladu s člankom 112. stavkom 1. UI akta, popis zabranjenih praksi u području umjetne inteligencije utvrđen u članku 5. UI akta i popis primjera upotrebe visokorizičnih sustava iz Priloga III. UI aktu podliježu godišnjem preispitivanju do kraja razdoblja delegiranja ovlasti iz članka 97. UI akta. Sljedeća procjena Komisije u skladu s člankom 112. UI akta stoga je predviđena za 2026., a Komisija će nakon dovršetka procjene svoje nalaze objaviti u izvješću.

(64) Kako bi se relevantni podaci dosljedno i sustavno prikupljali prije procjene za 2026., Komisija namjerava koordinirati stalno praćenje na nacionalnoj razini i razini EU-a. U tu će svrhu Ured za umjetnu inteligenciju surađivati s Vijećem za umjetnu inteligenciju i nacionalnim nadležnim tijelima država članica te će, prema potrebi, provoditi savjetovanja u okviru već uspostavljenih mehanizama suradnje nacionalnih kontaktnih točaka u relevantnim područjima. Posebna će se pozornost posvetiti područjima koja su označena za daljnje praćenje i prikupljanje dokaza u ovom izvješću. Međutim, pratit će se i tehnološki razvoj, kao i moguće relevantne promjene u upotrebi UI sustava, njihovi učinci i novi rizici.

(65) Prilikom procjene jesu li rizici povezani s umjetnom inteligencijom adekvatno obuhvaćeni postojećim zakonodavstvom EU-a, nakon što započne izvršavanje UI akta i stekne se praktično iskustvo, analizirat će se kakva je interakcija UI akta s drugim okvirima EU-a koji se bave rizikom za zdravlje, sigurnost i temeljna prava te kako ih dopunjuje. Posebna će se pozornost posvetiti usklađenosti i praktičnom međudjelovanju UI akta i instrumenata kao što su Akt o digitalnim uslugama, Akt o upravljanju podacima, Uredba o transparentnosti i ciljanju u političkom oglašavanju te pravna stečevina o zaštiti potrošača i slobodnom kretanju robe. Takvom bi se analizom trebalo nastojati utvrditi u kojoj se mjeri horizontalnim pravilima, sektorskim obvezama, mehanizmima upravljanja podacima i zaštitnim mjerama povezanima s proizvodima zajednički ublažavaju relevantni rizici te se na temelju toga donosi odluka je li potrebna daljnja regulatorna intervencija.