



EOVP-ENVP

**Skupno mnenje 4/2022
o predlogu uredbe
Evropskega parlamenta in
Sveta o določitvi pravil za
preprečevanje spolne zlorabe
otrok in boj proti njej**

Sprejeto 28. julija 2022

KAZALO VSEBINE

1.	Ozadje.....	7
2.	Obseg mnenja.....	8
3.	Splošne pripombe o pravicah do zaupnosti komunikacij in varstva osebnih podatkov.....	9
4.	Posebne pripombe	12
4.1	Razmerje z obstoječo zakonodajo.....	12
4.1.1	Razmerje z GDPR ter direktivo o zasebnosti in elektronskih komunikacijah	12
4.1.2	Razmerje z Uredbo (EU) 2021/1232 in vpliv na prostovoljno zaznavanje spolne zlorabe otrok na spletu	12
4.2	Zakonita podlaga po GDPR	13
4.3	Obveznosti v zvezi z ocenjevanjem in zmanjševanjem tveganja.....	13
4.4	Pogoji za izdajo odredb o zaznavanju	15
4.5	Analiza potrebnosti in sorazmernosti predvidenih ukrepov ()	16
4.5.1	Učinkovitost zaznavanja.....	17
4.5.2	Najmanj invaziven ukrep	18
4.5.3	Sorazmernost v ozkem pomenu	19
4.5.4	Zaznavanje znanih posnetkov spolne zlorabe otrok	21
4.5.5	Zaznavanje predhodno neznanih posnetkov spolne zlorabe otrok	21
4.5.6	Zaznavanje pridobivanja otrok za spolne namene	22
4.5.7	Ugotovitev o potrebnosti in sorazmernosti predvidenih ukrepov	23
4.6	Obveznosti naznanitve.....	24
4.7	Obveznosti odstranitve in blokiranja dostopa	24
4.8	Ustrezne tehnologije in zaščitni ukrepi	25
4.8.1	Vgrajeno in privzeto varstvo podatkov	25
4.8.2	Zanesljivost tehnologij	25
4.8.3	Pregledovanje zvočnih komunikacij	26
4.8.4	Preverjanje starosti	27
4.9	Ohranjanje informacij	27
4.10	Vpliv na šifriranje	27
4.11	Nadzor, izvrševanje in sodelovanje	29
4.11.1	Vloga nacionalnih nadzornih organov po GDPR.....	29
4.11.2	Vloga EOVP	30
4.11.3	Vloga Centra EU za boj proti spolni zlorabi otrok.....	31

4.11.4	Vloga Europol	33
5.	Sklepna ugotovitev	37

Povzetek

Evropska komisija je 11. maja 2022 objavila predlog uredbe Evropskega parlamenta in Sveta o določitvi pravil za preprečevanje spolne zlorabe otrok in boj proti njej.

Predlog bi ponudnikom storitev gostovanja, medosebnih komunikacijskih storitev in drugih storitev naložil določljive obveznosti glede zaznavanja, naznanjanja in odstranjevanja znanih in novih posnetkov spolne zlorabe otrok na spletu ter blokiranja dostopa do njih ter glede pridobivanja otrok za spolne namene. Poleg tega predlog določa vzpostavitev nove decentralizirane agencije EU (v nadaljevanju: Center EU) in mreže nacionalnih usklajevalnih organov za boj proti spolni zlorabi otrok, kar bo omogočilo izvajanje predlagane uredbe. Kot je ugotovljeno v obrazložitenem memorandumu k predlogu, bi ukrepi, ki jih vsebuje predlog, vplivali na uveljavljanje temeljnih pravic uporabnikov zadevnih storitev.

Spolna zloraba otrok je še posebej hudo in gnusno kaznivo dejanje, cilj omogočanja uspešnega ukrepanja za boj proti njej pa ustreza cilju splošnega interesa, ki ga priznava Unija, ter ima namen zavarovati pravice in svoboščine žrtev. EOVP in ENVP hkrati opozarjata, da morajo kakršne koli omejitve temeljnih pravic, kot so tiste, predvidene s predlogom, izpolnjevati zahteve iz člena 52(1) Listine Evropske unije o temeljnih pravicah.

EOVP in ENVP poudarjata, da predlog vzbuja resne pomisleke glede sorazmernosti predvidenega posega v varstvo temeljnih pravic do zasebnosti in varstva osebnih podatkov ter omejevanja varstva takih pravic. Glede tega poudarjata, da postopkovni zaščitni ukrepi ne morejo nikoli v celoti nadomestiti vsebinskih zaščitnih ukrepov. Zapleten sistem stopnjevanja od ukrepov za ocenjevanje in zmanjšanje tveganja do odredbe o zaznavanju ne more nadomestiti potrebne jasnosti vsebinskih obveznosti.

EOVP in ENVP menita, da predlogu manjka jasnost pri ključnih elementih, kot je pojem „znatno tveganje“. Poleg tega imajo subjekti, pristojni za uporabo teh zaščitnih ukrepov (od zasebnih subjektov do na koncu upravnih in/ali pravosodnih organov), zelo široko polje proste presoje, kar privede do pravne negotovosti glede načina uravnoteženja zadevnih pravic v posameznem primeru. EOVP in ENVP poudarjata, da mora zakonodajalec, kadar dovoli še posebej resne posege v temeljne pravice, zagotoviti pravno jasnost glede tega, kdaj in kje so posegi dovoljeni. Kljub zavedanju, da zakonodaja ne more biti preveč predpisujoča in da mora omogočati nekaj prožnosti pri njeni praktični uporabi, EOVP in ENVP menita, da zaradi neobstoja jasnih vsebinskih norm predlog pušča preveč prostora za morebitno zlorabo.

Kar zadeva potrebnost in sorazmernost predvidenih ukrepov za zaznavanje, sta EOVP in ENVP zlasti zaskrbljena, kadar gre za ukrepe, predvidene za zaznavanje neznanih posnetkov spolne zlorabe otrok in pridobivanja otrok za spolne namene v medosebnih komunikacijskih storitvah. Zaradi njihove invazivnosti, verjetnostne narave in stopenj napak, povezanih s takimi tehnologijami, EOVP in ENVP menita, da poseg, ki ga ustvarjajo navedeni ukrepi, presega tisto, kar je potrebno in sorazmerno. Poleg tega je verjetneje, da bodo ukrepi, ki javnim organom dovoljujejo splošen dostop do vsebine komunikacije, da se lahko zazna pridobivanje otrok za spolne namene, vplivali na bistveno vsebino pravic, zajamčenih v členih 7 in 8 Listine Evropske unije o temeljnih pravicah. Zato bi bilo treba ustrezne določbe, ki se nanašajo na pridobivanje otrok za spolne namene, odstraniti iz predloga. Poleg tega predlog iz svojega področja uporabe ne izključuje pregledovanja zvočnih komunikacij. EOVP in ENVP menita, da je pregledovanje zvočnih komunikacij še posebej invazivno in da mora kot tako ostati zunaj področja obveznosti zaznavanja, določenih v predlagani uredbi, tako v zvezi z glasovnimi sporočili kot tudi s komunikacijami v živo.

Poleg tega EOVP in ENVP izražata dvome v učinkovitost ukrepov za blokiranje dostopa ter menita, da bi bila zahteva, da ponudniki internetnih storitev dešifrirajo spletne komunikacije, da bi se lahko blokiral dostop do tistih, ki se nanašajo na posnetke spolne zlorabe otrok, nesorazmerna.

EOVP in ENVP še poudarjata, da tehnologije šifriranja bistveno pripomorejo k spoštovanju zasebnega življenja in zaupnosti komunikacij, svobodi izražanja ter inovacijam in rasti digitalnega gospodarstva, ki se opira na visoko raven zaupanja in zanesljivosti, ki jo zagotavljajo take tehnologije. V uvodni izjavi 26 predloga je tako v zvezi z izbiro tehnologije zaznavanja kot tudi tehničnimi ukrepi za varovanje zaupnosti komunikacij, kot je šifriranje, navedeno opozorilo, da mora navedena tehnološka izbira izpolnjevati zahteve predlagane uredbe, tj. da mora omogočiti zaznavanje. To gre v korist razumevanju, ki izhaja iz členov 8(3) in 10(2) predloga, da ponudnik ne more zavrniti izvršitve odredbe o zaznavanju na podlagi tehnične nezmožnosti. EOVP in ENVP menita, da bi morali biti družbeni potrebi po varnih in zasebnih komunikacijskih kanalih ter po boju proti njihovi zlorabi bolje uravnoteženi. V predlogu bi bilo treba jasno navesti, da se ničesar v predlagani uredbi ne bi smelo razlagati tako, da prepušča ali slabi šifriranje.

Čeprav EOVP in ENVP pozdravljata izjavo v predlogu, da ta ne vpliva na pooblastila in pristojnosti organov za varstvo podatkov iz Splošne uredbe o varstvu podatkov, menita, da bi bilo kljub temu treba bolj urediti razmerja med nalogami usklajevalnih organov in organov za varstvo podatkov. V zvezi s tem cenita vlogo, ki jo predlog dodeljuje EOVP, ko zahteva njegovo vključitev v praktično izvajanje predloga, zlasti potrebo, da EOVP izda mnenje o tehnologijah, ki bi jih Center EU dal na voljo za izvrševanje odredb o zaznavanju. Kljub temu bi bilo treba pojasniti, kakšen bi bil namen mnenja v postopku in kako bi Center EU ravnal po prejemu mnenja EOVP.

Nazadnje, EOVP in ENVP opozarjata, da predlog predvideva tesno sodelovanje med Centrom EU in Europolom, ki bi morala drug drugemu zagotoviti „čim bolj popoln dostop do ustreznih informacijskih sistemov“. Čeprav EOVP in ENVP načeloma podpirata sodelovanje navedenih agencij, pa glede na to, da Center EU ni organ kazenskega pregona, vendarle podajata več priporočil glede izboljšanja ustreznih določb, vključno s tem, da prenos podatkov med Centrom EU in Europolom poteka le prek komunikacijskega orodja za varno izmenjavo, kot je omrežje SIENA, za vsak primer posebej in na podlagi ustrezno ocenjene zahteve.

Evropski odbor za varstvo podatkov in Evropski nadzornik za varstvo podatkov sta,

ob upoštevanju člena 42(2) Uredbe 2018/1725 z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (v nadaljevanju: uredba EUDPR),¹

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018,²

ob upoštevanju zahteve Evropske komisije za skupno mnenje Evropskega odbora za varstvo podatkov in Evropskega nadzornika za varstvo podatkov z dne 12. maja 2022 o predlogu uredbe Evropskega parlamenta in Sveta o določitvi pravil za preprečevanje spolne zlorabe otrok in boj proti njej,³

SPREJELA NASLEDNJE SKUPNO MNENJE

1. OZADJE

1. Evropska komisija (v nadaljevanju: Komisija) je 11. maja 2022 objavila predlog uredbe Evropskega parlamenta in Sveta o določitvi pravil za preprečevanje spolne zlorabe otrok in boj proti njej (v nadaljevanju: predlog ali predlagana uredba).⁴
2. Predlog je bil izdan po sprejetju Uredbe (EU) 2021/1232 o začasnem odstopanju od nekaterih določb Direktive 2002/58/ES glede uporabe tehnologij s strani ponudnikov medosebnih komunikacijskih storitev, neodvisnih od številke, za obdelavo osebnih in drugih podatkov za namene boja proti spolni zlorabi otrok na spletu (v nadaljevanju: začasna uredba)⁵. V skladu z začasno uredbo zadevnim ponudnikom storitev ni treba vzpostaviti ukrepov za zaznavanje posnetkov spolne zlorabe otrok (na primer fotografij in videoposnetkov) ali pridobivanja otrok za spolne namene v okviru svojih storitev, temveč je tem ponudnikom omogočeno, da to storijo prostovoljno v skladu s pogoji iz navedene uredbe.⁶
3. Predlog je sestavljen iz dveh glavnih elementov. Prvič, predlog ponudnikom storitev gostovanja, medosebnih komunikacijskih storitev in drugih storitev nalaga določene obveznosti glede zaznavanja, naznanjanja in odstranjevanja znanih in novih posnetkov spolne zlorabe otrok na spletu ter blokiranja

¹ UL L 295, 21. 11. 2018, str. 39.

² Omenjanje „državčanic“ v tem dokumentu je treba razumeti kot omenjanje „državčanic EGP“.

³ Predlog uredbe Evropskega parlamenta in Sveta o določitvi pravil za preprečevanje spolne zlorabe otrok in boj proti njej, COM(2022) 209 final.

⁴ Prav tam.

⁵ Uredba (EU) 2021/1232 Evropskega parlamenta in Sveta z dne 14. julija 2021 o začasnem odstopanju od nekaterih določb Direktive 2002/58/ES glede uporabe tehnologij s strani ponudnikov medosebnih komunikacijskih storitev, neodvisnih od številke, za obdelavo osebnih in drugih podatkov za namene boja proti spolni zlorabi otrok na spletu, UL [2021] L 274/41.

⁶ Glej tudi Mnenje 7/2020 Evropskega nadzornika za varstvo podatkov o predlogu za začasna odstopanja od Direktive 2002/58/ES za namene boja proti spolni zlorabi otrok na spletu (10. november 2020).

dostopa do njih ter glede pridobivanja otrok za spolne namene. Drugič, predlog določa vzpostavitev nove decentralizirane agencije EU (v nadaljevanju: Center EU za boj proti spolni zlorabi otrok ali Center EU) in mreže nacionalnih usklajevalnih organov za boj proti spolni zlorabi otrok, kar bo omogočilo izvajanje predlagane uredbe.⁷

4. Kot je ugotovljeno v obrazložitvenem memorandumu k predlogu, bi ukrepi, ki jih vsebuje predlog, vplivali na uveljavljanje temeljnih pravic uporabnikov zadevnih storitev. Te pravice vključujejo zlasti temeljne pravice do spoštovanja zasebnosti (vključno z zaupnostjo komunikacij, kar je del širše pravice do spoštovanja zasebnega in družinskega življenja), varstva osebnih podatkov ter svobode izražanja in obveščanja.⁸
5. Poleg tega je namen takih predlaganih ukrepov nadgraditi ter deloma dopolniti veljavno zakonodajo EU o varstvu podatkov in zasebnosti. V zvezi s tem je v obrazložitvenem memorandumu ugotovljeno naslednje:

„Predlog temelji na Splošni uredbi o varstvu podatkov. Ponudniki se v praksi pri obdelavi osebnih podatkov, ki so neločljivo povezani s prostovoljnim zaznavanjem in naznanjanjem spolne zlorabe otrok na spletu, navadno sklicujejo na različne razloge za obdelavo, določene v Splošni uredbi o varstvu podatkov. Predlog določa sistem ciljno usmerjenih odredb o zaznavanju in pogoje za zaznavanje, kar zagotavlja večjo pravno varnost za navedene dejavnosti. Kar zadeva obvezne dejavnosti zaznavanja, ki vključujejo obdelavo osebnih podatkov, predlog, zlasti odredbe o zaznavanju, izdane na podlagi njega, vzpostavlja podlago za tako obdelavo iz člena 6(1), točka (c) Splošne uredbe o varstvu podatkov, ki določa obdelavo osebnih podatkov, potrebno za izpolnitev zakonske obveznosti po pravu Unije ali države članice, ki velja za upravljavca.

Predlog med drugim zajema ponudnike, ki ponujajo elektronske medosebne komunikacijske storitve ter so zato podvrženi nacionalnim določbam o izvajanju direktive o zasebnosti in elektronskih komunikacijah in njene predlagane revizije, o kateri trenutno potekajo pogajanja. Ukrepi, navedeni v predlogu, v nekaterih pogledih omejujejo obseg pravic in obveznosti na podlagi ustreznih določb navedene direktive, in sicer v zvezi z dejavnostmi, ki so nujno potrebne za izvršitev odredb o zaznavanju. V zvezi s tem predlog po analogiji vključuje uporabo člena 15(1) navedene direktive.“⁹

6. Glede na resnost predvidenih posegov v temeljne pravice je predlog še zlasti pomemben za varstvo pravic in svoboščin posameznikov pri obdelavi osebnih podatkov. Tako se je Evropska komisija 12. maja 2022 odločila, da se v skladu s členom 42(2) uredbe EUDPR posvetuje z Evropskim odborom za varstvo podatkov (v nadaljevanju: EOVP) in Evropskim nadzornikom za varstvo podatkov (v nadaljevanju: ENVP).

2. OBSEG MNENJA

7. V tem skupnem mnenju so podana skupna stališča EOVP in ENVP o predlogu. Omejeno je na vidike predloga, ki se nanašajo na varstvo zasebnosti in osebnih podatkov. Skupno mnenje zlasti poudarja področja, na katerih predlog ne zagotavlja zadostnega varstva temeljnih pravic do zasebnosti in

⁷ COM(2022) 209 final, str. 17.

⁸ COM(2022) 209 final, str. 12.

⁹ COM(2022) 209 final, str. 4–5.

varstva podatkov ali na katerih ga je treba dodatno uskladiti s pravnim okvirom EU za varstvo zasebnosti in osebnih podatkov.

8. Kakor je pojasnjeno v nadaljevanju tega skupnega mnenja, predlog vzbuja resne pomisleke glede potrebnosti in sorazmernosti predvidenih posegov v varstvo temeljnih pravic do zasebnosti in varstva osebnih podatkov ter omejevanja varstva teh pravic. Kljub temu namen tega skupnega mnenja ni podati izčrpnega seznama vseh težav glede zasebnosti in varstva podatkov, ki jih prinaša predlog, ali konkretnih predlogov za izboljšanje besedila predloga. Namesto tega so v tem skupnem mnenju podane pripombe o glavnih težavah, ki jih prinaša predlog in ki sta jih ugotovila EOVP in ENVP, na visoki ravni. EOVP in ENVP sta kljub temu še vedno na voljo za podajanje dodatnih pripomb in priporočil zakonodajalcema v okviru zakonodajnega postopka v zvezi s postopkom.

3. SPLOŠNE PRIPOMBE O PRAVICAH DO ZAUPNOSTI KOMUNIKACIJ IN VARSTVA OSEBNIH PODATKOV

9. Zaupnost komunikacij je bistven element temeljne pravice do spoštovanja zasebnega in družinskega življenja, kakor je določeno v členu 7 Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina).¹⁰ Poleg tega je v členu 8 Listine priznana temeljna pravica do varstva osebnih podatkov. Prav tako so pravice do zaupnosti komunikacij ter pravica do zasebnega in družinskega življenja zajamčene v členu 8 Evropske konvencije o človekovih pravicah in so sestavni del ustavnih tradicij, skupnih državam članicam.¹¹
10. EOVP in ENVP opozarjata, da pravice, določene v členih 7 in 8 Listine, niso absolutne pravice, temveč jih je treba upoštevati glede na njihovo funkcijo v družbi.¹² Spolna zloraba otrok je še posebej hudo in gnusno kaznivo dejanje, cilj omogočanja uspešnega ukrepanja za boj proti njej pa ustreza cilju splošnega interesa, ki ga priznava Unija, ter ima namen zavarovati pravice in svoboščine žrtev. Kar zadeva učinkovit boj proti kaznivim dejanjem, katerih žrtve so mladoletniki in druge ranljive osebe, je Sodišče Evropske unije (v nadaljevanju: Sodišče) poudarilo, da iz člena 7 Listine lahko izhajajo pozitivne obveznosti za javne organe, da sprejmejo pravne ukrepe za zavarovanje zasebnega in družinskega življenja, stanovanja ter komunikacij. Take obveznosti lahko izhajajo tudi iz členov 3 in 4 Listine v zvezi z varstvom telesne in duševne celovitosti oseb ter prepovedjo mučenja in nečlovečnega in ponižujočega ravnanja.¹³
11. Hkrati morajo kakršne koli omejitve z Listino zajamčenih pravic, kot so tiste, predvidene s predlogom,¹⁴ izpolnjevati zahteve iz člena 52(1) Listine. Vsak ukrep, ki posega v pravico do zaupnosti komunikacij

¹⁰ Glej na primer Izjavo Evropskega odbora za varstvo podatkov o spremembi Uredbe o e-zasebnosti in njenem učinku na varstvo posameznikov glede zasebnosti in zaupnosti njihovih komunikacij (25. maj 2018).

¹¹ Skoraj vse evropske ustave vključujejo pravico do varstva zaupnosti komunikacij. Glej na primer 15. člen Ustave Italijanske republike; 10. člen Temeljnega zakona Zvezne republike Nemčije; 22. člen Belgijske ustave in 13. člen Ustave Kraljevine Nizozemske.

¹² Glej med drugim sodbo Sodišča z dne 16. julija 2020, *Facebook Ireland in Schrems*, C-311/18, točka 172 in navedena sodna praksa. Glej tudi uvodno izjavo 4 k Splošni uredbi o varstvu podatkov.

¹³ Sodba Sodišča z dne 6. oktobra 2020, *La Quadrature du Net in drugi*, združene zadeve C-511/18, C-512/18 in C-520/18, točke 126–128. Glej tudi Mnenje 7/2020 Evropskega nadzornika za varstvo podatkov o predlogu začasna odstopanja od Direktive 2002/58/ES za namene boja proti spolni zlorabi otrok na spletu (10. november 2020), točka 12.

¹⁴ Glej COM(2022) 209 final, str. 12–13.

ter pravico do zasebnega in družinskega življenja, mora najprej spoštovati bistveno vsebino zadevnih pravic in svoboščin.¹⁵ Do vpliva na bistveno vsebino pravice pride, če je osnovna vsebina pravice izpraznjena in posameznik pravice ne more uveljaviti¹⁶. Glede na postavljeni cilj poseg ne sme pomeniti tako nesorazmernega in nedopustnega posredovanja, ki bi posegalo v samo bistvo tako zagotovljene pravice.¹⁷ To pomeni, da ima celo temeljna pravica, ki po naravi ni absolutna, kot sta pravica do zaupnosti komunikacij in pravica do varstva osebnih podatkov, nekatere osrednje sestavine, ki jih ni dopustno omejiti.

12. Sodišče je na področju zasebnosti elektronskih komunikacij večkrat uporabilo preizkus „bistvene vsebine pravice“. V zadevi *Tele2 Sverige in Watson* je odločilo, da ureditev, ki ne dovoljuje hrambe vsebine komunikacije, ni taka, da bi škodovala bistveni vsebini pravic do zasebnega življenja in varstva osebnih podatkov.¹⁸ Sodišče je v zadevi *Schrems* ugotovilo, da je treba šteti, da ureditev, ki javnim organom omogoča splošen dostop do vsebine elektronskih komunikacij, pomeni poseg v bistveno vsebino temeljne pravice do spoštovanja zasebnega življenja, kot je zagotovljena v členu 7 Listine.¹⁹ Sodišče je v zadevi *Digital Rights Ireland in Seitlinger in drugi* ugotovilo, da čeprav je hramba podatkov, določena z Direktivo 2006/24, pomenila posebej resno poseganje v temeljno pravico do spoštovanja zasebnega življenja in drugih pravic, potrjenih v členu 7 Listine, ni mogla posegati v bistveno vsebino teh pravic, saj ta direktiva ni dovoljevala seznanjanja z vsebino elektronskih komunikacij kot tako.²⁰ Na podlagi te sodne prakse je mogoče sklepati, da je verjetneje, da bodo ukrepi, ki javnim organom dovoljujejo splošen dostop do vsebine komunikacije, vplivali na bistveno vsebino pravic, zajamčenih v členih 7 in 8 Listine. Ti premisleki so enako pomembni tudi v zvezi z ukrepi za zaznavanje posnetkov spolne zlorabe otrok in pridobivanja otrok za spolne namene, kot so ti, predvideni s predlogom.
13. Poleg tega je Sodišče ugotovilo, da imajo ukrepi za varnost podatkov ključno vlogo pri zagotavljanju, da ni poseganja v bistveno vsebino temeljne pravice do varstva podatkov iz člena 8 Listine.²¹ V digitalni dobi so tehnične rešitve za zavarovanje in zaščito zaupnosti elektronskih komunikacij, vključno z ukrepi za šifriranje, ključne za zagotavljanje uživanja vseh temeljnih pravic.²² To bi bilo treba ustrezno upoštevati pri ocenjevanju ukrepov za obvezno zaznavanje posnetkov spolne zlorabe otrok ali pridobivanja otrok za spolne namene, zlasti če bi privedli do oslabitve ali poslabšanja šifriranja.²³
14. Poleg tega člen 52(1) Listine določa, da mora biti kakršno koli omejevanje uresničevanja v Listini zajamčene temeljne pravice predpisano z zakonom. Ob upoštevanju načela sorazmernosti so omejitve dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava

¹⁵ Člen 52(1) Listine.

¹⁶ Glej EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (Smernice ENVP za ocenjevanje sorazmernosti ukrepov, ki omejujejo temeljne pravice do zasebnosti in varstva osebnih podatkov) (19. december 2019), str. 8, na voljo na https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

¹⁷ Sodba Sodišča z dne 14. januarja 2021, OM, C-393/19, točka 53.

¹⁸ Sodba Sodišča z dne 21. decembra 2016, *Tele2 Sverige in Watson*, združeni zadevi C-203/15 in C-698/15, točka 101.

¹⁹ Sodba Sodišča z dne 6. oktobra 2015, *Schrems*, C-362/14, točka 94.

²⁰ Sodba Sodišča z dne 8. aprila 2014, *Digital Rights Ireland in Seitlinger in drugi*, združeni zadevi C-293/12 in C-594/12, točka 39.

²¹ Prav tam, točka 40.

²² Glej Resolucijo 47/16 Sveta za človekove pravice o spodbujanju, varstvu in uživanju človekovih pravic na internetu, dokument ZNA/HRC/RES/47/16 (26. julij 2021).

²³ Glej tudi uvodno izjavo 25 začasne uredbe.

Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.²⁴ Za izpolnitev zahteve po sorazmernosti mora ureditev določati jasna in natančna pravila, ki urejajo obseg in uporabo zadevnih ukrepov ter določajo minimalne zahteve, tako da imajo osebe, za osebne podatke katerih gre, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje teh podatkov pred tveganji zlorabe.²⁵ V tej ureditvi mora biti navedeno, v kakšnih okoliščinah in pod katerimi pogoji je mogoče sprejeti ukrep, ki določa obdelavo takih podatkov, s čimer se tako zagotovi, da je poseganje omejeno na to, kar je nujno potrebno.²⁶ Kot je pojasnilo Sodišče, je nujnost obstoja takih jamstev toliko pomembnejša, kadar se osebni podatki obdelujejo avtomatizirano in kadar gre za varstvo posebne kategorije osebnih podatkov, ki so občutljivi podatki.²⁷

15. Predlog bi izvajanje pravic in obveznosti, določenih v členih 5(1) in (3) ter 6(1) Direktive 2002/58/ES (v nadaljevanju: direktiva o zasebnosti in elektronskih komunikacijah)²⁸, omejil, kolikor je potrebno za izvrševanje odredb o zaznavanju, izdanih v skladu z oddelkom 2 poglavja 1 predloga. EOVP in ENVP menita, da je zato treba predlog oceniti ne le z vidika Listine in Splošne uredbe o varstvu podatkov, temveč tudi z vidika členov 5 in 6 ter člena 15(1) direktive o zasebnosti in elektronskih komunikacijah.

²⁴ Glej Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Tool kit (Ocenjevanje potrebnosti ukrepov, ki omejujejo temeljno pravico do varstva osebnih podatkov: zbirka orodij), 11. april 2019, https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

²⁵ Sodba Sodišča z dne 6. oktobra 2020, *La Quadrature du Net in drugi*, združene zadeve C-511/18, C-512/18 in C-520/18, točka 132.

²⁶ Prav tam.

²⁷ Prav tam.

²⁸ Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), kakor je bila spremenjena z Direktivo 2006/24/ES in Direktivo 2009/136/ES.

4. POSEBNE PRIPOMBE

4.1 Razmerje z veljavno zakonodajo

4.1.1 Razmerje s Splošno uredbo o varstvu podatkov ter direktivo o zasebnosti in elektronskih komunikacijah

16. V predlogu je navedeno, da ne posega v pravila, ki izhajajo iz drugih aktov Unije, zlasti Splošne uredbe o varstvu podatkov²⁹ ter direktive o zasebnosti in elektronskih komunikacijah. V nasprotju z začasno uredbo predlog ne določa izrecnega začasnega odstopanja od direktive o zasebnosti in elektronskih komunikacijah, temveč omejitev izvajanja pravic in obveznosti iz členov 5(1), 5(3) in 6(1) direktive o zasebnosti in elektronskih komunikacijah. Poleg tega je treba opozoriti, da začasna uredba določa odstopanje le od določb členov 5(1) in 6(1), ne pa od člena 5(3) direktive o zasebnosti in elektronskih komunikacijah.
17. Predlog omenja tudi člen 15(1) direktive o zasebnosti in elektronskih komunikacijah, ki državam članicam dovoljuje sprejetje zakonskih ukrepov, s katerimi omejijo obseg pravic in obveznosti, določenih v členih 5 in 6 navedene direktive, kadar taka omejitev pomeni potreben, primeren in ustrezen ukrep v demokratični družbi za, med drugim, preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj. V skladu s predlogom se člen 15(1) direktive o zasebnosti in elektronskih komunikacijah uporablja po analogiji, pri čemer predlog omejuje izvajanje pravic in obveznosti iz členov 5(1), 5(3) in 6(1) direktive o zasebnosti in elektronskih komunikacijah.
18. EOVP in ENVP opozarjata, da je Sodišče pojasnilo, da je treba člen 15(1) direktive o zasebnosti in elektronskih komunikacijah razlagati ozko, kar pomeni, da mora izjemati od načela zaupnosti komunikacij, ki jo dovoljuje člen 15(1), ostati izjema in ne sme postati pravilo.³⁰ Kakor je opisano v nadaljevanju tega skupnega mnenja, EOVP in ENVP menita, da predlog ne izpolnjuje zahtev (nujne) potrebnosti, učinkovitosti in sorazmernosti. Poleg tega EOVP in ENVP ugotavljata, da bi po predlogu poseg v zaupnost komunikacij dejansko lahko postal pravilo in ne bi ostal izjema.

4.1.2 Razmerje z Uredbo (EU) 2021/1232 in vpliv na prostovoljno zaznavanje spolne zlorabe otrok na spletu

19. V skladu s členom 88 predloga bi ta razveljavil začasno uredbo, ki določa začasno odstopanje od nekaterih določb direktive o zasebnosti in elektronskih komunikacijah, da se omogoči prostovoljna uporaba tehnologij za zaznavanje posnetkov spolne zlorabe otrok in pridobivanja otrok za spolne namene s strani ponudnikov medosebnih komunikacijskih storitev, neodvisnih od številke. Tako od dneva začetka uporabe predlagane uredbe ne bi bilo odstopanja od direktive o zasebnosti in elektronskih komunikacijah, ki bi dovoljevalo prostovoljno zaznavanje spolne zlorabe otrok na spletu s strani takih ponudnikov.
20. Ker bi obveznosti zaznavanja, ki jih uvaja predlog, veljale le za prejemnike odredb o zaznavanju, bi bilo v besedilu predlagane uredbe pomembno pojasniti, da prostovoljna uporaba tehnologij za zaznavanje

²⁹ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Besedilo velja za EGP), UL L 119, 4. 5. 2016, str. 1–88.

³⁰ Sodba Sodišča z dne 21. decembra 2016, *Tele2 Sverige AB in Watson*, združeni zadevi C-203/15 in C-698/15, točka 89.

posnetkov spolne zlorabe otrok in pridobivanja otrok za spolne namene ostaja dovoljena le, če jo dovoljujeta direktiva o zasebnosti in elektronskih komunikacijah ter Splošna uredba o varstvu podatkov. To bi na primer pomenilo, da bi bila ponudnikom medosebnih komunikacijskih storitev, neodvisnih od številke, preprečena prostovoljna uporaba takih tehnologij, razen če bi to dovoljevala nacionalna zakonodaja, s katero se prenaša direktiva o zasebnosti in elektronskih komunikacijah, v skladu s členom 15(1) direktive o zasebnosti in elektronskih komunikacijah ter Listino.

21. Splošneje, za predlagano uredbo bi bilo dobro, če bi se dodatno pojasnila status prostovoljnega zaznavanja spolne zlorabe otrok na spletu po datumu začetka uporabe predlagane uredbe ter prehod s sistema prostovoljnega zaznavanja iz začasne uredbe na obveznosti zaznavanja iz predlagane uredbe. EOVP in ENVP denimo priporočata, da se pojasni, da predlagana uredba ne bi določala zakonite podlage za obdelavo osebnih podatkov izključno za namen prostovoljnega zaznavanja spolne zlorabe otrok na spletu.

4.2 Zakonita podlaga po Splošni uredbi o varstvu podatkov

22. Namen predloga je vzpostaviti zakonito podlago v smislu Splošne uredbe o varstvu podatkov za obdelavo osebnih podatkov za zaznavanje posnetkov spolne zlorabe otrok in pridobivanja otrok za spolne namene. V skladu s tem je v obrazložitvenem memorandumu ugotovljeno naslednje: „Kar zadeva obvezne dejavnosti zaznavanja, ki vključujejo obdelavo osebnih podatkov, predlog, zlasti odredbe o zaznavanju, izdane na podlagi njega, vzpostavlja podlago za tako obdelavo iz člena 6(1), točka (c), Splošne uredbe o varstvu podatkov, ki določa obdelavo osebnih podatkov, potrebno za izpolnitev zakonske obveznosti po pravu Unije ali države članice, ki velja za upravljavca.“³¹
23. EOVP in ENVP pozdravljata odločitev Komisije, da odpravi pravno negotovost glede pravne podlage za obdelavo osebnih podatkov, ki izhaja iz začasne uredbe. EOVP in ENVP se tudi strinjata z ugotovitvijo Komisije, da so posledice uvedbe ukrepov za zaznavanje preveč daljnosežne in resne, da bi se odločanje o izvajanju takih ukrepov prepuščalo ponudnikom storitev.³² Hkrati EOVP in ENVP opozarjata, da bo katera koli pravna podlaga, ki ponudnike storitev zavezuje k poseganju v temeljne pravice do varstva podatkov in zasebnosti, veljavna le, če bo upoštevala pogoje iz člena 52(1) Listine, kakor so preučeni v naslednjih oddelkih.

4.3 Obveznosti v zvezi z ocenjevanjem in zmanjševanjem tveganja

24. V skladu z oddelkom 1 poglavja II predloga morajo ponudniki storitev gostovanja in medosebnih komunikacijskih storitev za vsako tako storitev, ki jo ponujajo, opredeliti, analizirati in oceniti tveganje uporabe storitve za namene spolne zlorabe otrok na spletu, nato pa z uporabo razumnih ukrepov za zmanjšanje tveganja, ki so prilagojeni ugotovljenemu tveganju, poskušati ugotovljeno tveganje karseda zmanjšati.
25. EOVP in ENVP opozarjata, da bi ponudnik pri izvajanju ocene tveganja moral upoštevati zlasti elemente, navedene v členu 3(2)(a) do (e) predloga, vključno s: prepovedmi in omejitvami, navedenimi v pogojih poslovanja ponudnika; načinom, kako uporabniki uporabljajo storitev, in njegovim vplivom na navedeno tveganje; načinom, kako je ponudnik zasnoval in upravlja storitev, vključno s poslovnim modelom, upravljanjem ter ustreznimi sistemi in postopki, ter vplivom na navedeno tveganje. V zvezi s tveganjem za pridobivanje otrok za spolne namene bi bilo treba upoštevati naslednje predlagane elemente: obseg, v katerem storitev uporabljajo ali jo bodo verjetno

³¹ Prav tam, str. 4.

³² Glej predlog, COM(2022) 209 final, str. 14.

uporabljali otroci; starostne skupine in tveganje za pridobivanje otrok za spolne namene po starostnih skupinah; razpoložljivost funkcionalnosti, ki omogočajo iskanje uporabnikov, funkcionalnosti, ki uporabnikom omogočajo, da neposredno vzpostavijo stik z drugimi uporabniki, zlasti prek zasebnih komunikacij, ter funkcionalnosti, ki uporabnikom omogočajo, da delijo slike ali videoposnetke z drugimi uporabniki.

26. Čeprav EOVP in ENVP priznavata, da se ta merila zdijo ustrezna, sta kljub temu zaskrbljena, da bi taka merila omogočila precej široko polje proste presoje in razlage. Več meril je opisanih z zelo splošnimi izrazi (na primer „način, kako uporabniki uporabljajo storitev, in njegov vpliv na navedeno tveganje“) ali se nanašajo na osnovne funkcionalnosti, ki so skupne številnim spletnim storitvam (na primer „omogočanje uporabnikom, da delijo slike ali videoposnetke z drugimi uporabniki“). Za merila kot taka se zdi, da so dovzetna za subjektivno (in ne objektivno) oceno.
27. Po mnenju EOVP in ENVP enako velja za ukrepe za zmanjšanje tveganja, ki bi jih bilo treba sprejeti v skladu s členom 4 predloga. Ukrepi, kot so prilagajanje ponudnikovih sistemov za moderiranje vsebine ali priporočilnih sistemov z ustreznimi tehničnimi in operativnimi ukrepi ter kadrovanjem, se zdijo pomembni za zmanjševanje ugotovljenega tveganja. Kljub temu pa ta merila pri uporabi v zapletenem postopku ocenjevanja tveganja ter skupaj z abstraktnimi in nejasnimi pojmi, ki opisujejo sprejemljivo količino tveganja (na primer „precejšnja mera“), ne ustrezajo merilom pravne varnosti in predvidljivosti, kar je potrebno za upravičenje posega v zaupnost komunikacij med fizičnimi osebami, ki pomeni jasen poseg v temeljne pravice do zasebnosti in svobode izražanja.
28. Čeprav ponudniki niso pooblašteni, da v okviru svojih strategij ocenjevanja in zmanjševanja tveganja posegajo v zaupnost komunikacij pred prejemom odredbe o zaznavanju, obstaja neposredna povezava med obveznostmi ocenjevanja in zmanjševanja tveganja ter posledičnimi obveznostmi zaznavanja. V skladu s členom 7(4) predloga je izdaja odredbe o zaznavanju odvisna od obstoja dokazov o znatnem tveganju, da bi zadevna storitev lahko bila uporabljena za namene spolne zlorabe otrok na spletu. Pred izdajo odredbe o zaznavanju je treba izvesti zapleten postopek, ki vključuje ponudnike, usklajevalni organ ter pravosodni ali drug neodvisni upravni organ, pristojen za izdajo odredbe. Ponudniki morajo najprej oceniti tveganje za uporabo njihovih storitev za namene spolne zlorabe otrok na spletu (člen 3 predloga) ter oceniti mogoče ukrepe za zmanjšanje tveganja (člen 4 predloga). Rezultati tega postopka se nato sporočijo pristojnemu usklajevalnemu organu (člen 5 predloga). Če ocena tveganja pokaže, da znatno tveganje ostaja kljub prizadevanjem za njegovo zmanjšanje, usklajevalni organ ponudnika zasliši glede osnutka zahteve za izdajo odredbe o zaznavanju in mu omogoči, da predloži pripombe. Ponudnik je nato dolžan predložiti izvedbeni načrt, vključno z mnenjem pristojnega organa za varstvo podatkov v primeru zaznavanja pridobivanja otrok za spolne namene. Če usklajevalni organ nadaljuje postopek, zaprosi za odredbo o zaznavanju, ki jo na koncu izda sodišče ali drug neodvisen upravni organ. Tako so začetna ocena tveganja in ukrepi, izbrani za zmanjšanje ugotovljenega tveganja, odločilni za oceno usklajevalnega organa in pristojnega pravosodnega ali upravnega organa glede potrebnosti odredbe o zaznavanju.
29. EOVP in ENVP ugotavljata, da so koraki, ki privedejo do izdaje odredbe o zaznavanju, zapleteni, saj vključujejo začetno ponudnikovo oceno tveganja in ponudnikov predlog za ukrepe za zmanjšanje tveganja ter nadaljnje stike ponudnika s pristojnim usklajevalnim organom. EOVP in ENVP menita, da obstaja precejšnja možnost, da bo ponudnik vplival na izid postopka. Glede tega opozarjata, da uvodna izjava 17 predloga določa, da bi morali ponudniki v okviru poročanja o tveganjih imeti možnost navesti „svojo pripravljenost“ na morebitni prejem odredbe o zaznavanju. Zato ni mogoče domnevati, da se bo prav vsak ponudnik poskušal izogniti odredbi o zaznavanju, da bi z uporabo najučinkovitejših in hkrati najmanj invazivnih ukrepov za zmanjšanje tveganja ohranil zaupnost komunikacij svojih

uporabnikov, zlasti če taki ukrepi za zmanjšanje tveganja posegajo v ponudnikovo svobodo gospodarske pobude v skladu s členom 16 Listine.

30. EOVP in ENVP želita poudariti, da postopkovni zaščitni ukrepi ne morejo nikoli v celoti nadomestiti vsebinskih zaščitnih ukrepov. Zato bi opisani zapleteni postopek, ki privede do mogoče izdaje odredbe o zaznavanju, morale spremljati jasne vsebinske obveznosti. EOVP in ENVP menita, da predlogu manjka jasnost pri več ključnih elementih (na primer pri pojmih „znatno tveganje“ in „precejšnja mera“), česar ni mogoče odpraviti z obstojem več ravni postopkovnih zaščitnih ukrepov. To je še pomembnejše z vidika dejstva, da imajo subjekti, pristojni za uporabo teh zaščitnih ukrepov (na primer ponudniki in pravosodni organi), široko polje proste presoje glede načina uravnoteženja zadevnih pravic v posameznem primeru. Z vidika obsežnih posegov v temeljne pravice, ki bi izhajali iz sprejetja predloga, bi zakonodajalec moral poskrbeti, da predlog zagotovi več jasnosti glede tega, kdaj in kje so taki posegi dovoljeni. Kljub zavedanju, da zakonodajni ukrepi ne morejo biti preveč predpisujoči in da morajo omogočati nekaj prožnosti pri njihovi praktični uporabi, EOVP in ENVP menita, da zaradi neobstoja jasnih vsebinskih norm sedanje besedilo predloga pušča preveč prostora za morebitno zlorabo.
31. Glede na mogoč znaten vpliv na zelo veliko število posameznikov, na katere se nanašajo osebni podatki (tj. na potencialno vse uporabnike medosebnih komunikacijskih storitev), EOVP in ENVP poudarjata potrebo po pravni varnosti, jasnosti in predvidljivosti zakonodaje na visoki ravni, s čimer bi se zagotovilo, da so predlagani ukrepi dejansko učinkoviti pri doseganju postavljenega cilja ter hkrati najmanj škodljivi za zadevne temeljne pravice.

4.4 Pogoji za izdajo odredb o zaznavanju

32. Člen 7 predloga določa, da bo usklajevalni organ v državi sedeža pooblaščen, da od pristojnega pravosodnega organa ali drugega neodvisnega upravnega organa navedene države članice zahteva, naj izda odredbo o zaznavanju, s katero od ponudnika storitev gostovanja ali medosebnih komunikacijskih storitev zahteva, da sprejme ukrepe iz člena 10 za zaznavanje spolne zlorabe otrok na spletu v specifični storitvi.
33. EOVP in ENVP ustrezno upoštevata, da bodo pred izdajo odredbe o zaznavanju izpolnjeni naslednji elementi:
- a. obstajajo dokazi o znatnem tveganju uporabe storitve za namene spolne zlorabe otrok na spletu v smislu odstavkov 5, 6 in 7 člena 7, kot je ustrezno;
 - b. razlogi za izdajo odredbe o zaznavanju prevladajo nad negativnimi posledicami za pravice in zakonite interese vseh prizadetih strani, zlasti ob upoštevanju potrebe po zagotovitvi pravičnega ravnesja med temeljnimi pravicami navedenih strani.
34. Pomen znatnega tveganja je opredeljen v odstavku 5 in naslednjih odstavkih člena 7 glede na vrsto odredbe o zaznavanju, ki se obravnava. Domneva se, da pri odredbah o zaznavanju v zvezi z zaznavanjem znanih posnetkov spolne zlorabe otrok obstaja znatno tveganje, če:
- a. se storitev kljub vsem ukrepom za zmanjšanje tveganja, ki jih je ponudnik morda sprejel ali jih bo sprejel, verjetno pretežno uporablja za razširjanje znanih posnetkov spolne zlorabe otrok; in
 - b. obstajajo dokazi, da se je storitev ali primerljiva storitev, če storitev na dan zahteve za izdajo odredbe o zaznavanju še ni bila ponujena v Uniji, v zadnjih 12 mesecih pretežno uporabljala za razširjanje znanih posnetkov spolne zlorabe otrok.

35. Da bi se lahko izdala odredba o zaznavanju neznanih posnetkov spolne zlorabe otrok, se morajo verjetnost in dejanski dokazi nanašati na neznane posnetke spolne zlorabe otrok, pred tem pa mora biti izdana odredba o zaznavanju znanih posnetkov spolne zlorabe otrok, ki je privedla do številnih ponudnikovih naznanitev v zvezi z znanimi posnetki spolne zlorabe otrok (člen 7(6) predloga). Kar zadeva odredbo o zaznavanju pridobivanja otrok za spolne namene, se bo štel, da znatno tveganje obstaja, če je ponudnik opredeljen kot ponudnik medosebnih komunikacijskih storitev, se storitev verjetno pretežno uporablja za pridobivanje otrok za spolne namene in obstajajo dokazi, da se je storitev pretežno uporabljala za pridobivanje otrok za spolne namene (člen 7(7) predloga).
36. EOVP in ENVP ugotavljata, da kljub opredelitvam v členu 7(5)–(7) predloga pri pogojih za izdajo odredbe o zaznavanju prevladujejo nejasni pravni pojmi, kot sta „pretežno“ in „številni“, pogoji pa se deloma ponavljajo, saj bodo dokazi o pretekli zlorabi pogosto pripomogli k ugotavljanju verjetnosti prihodnje zlorabe.
37. Predlog predvideva sistem, po katerem je treba pri odločanju o potrebnosti odredbe o zaznavanju sprejeti odločitev, s katero se predvidi prihodnja uporaba storitve za spolno zlorabo otrok na spletu. Zato je razumljivo, da je narava elementov iz člena 7 prognostična. Uporaba nejasnih pojmov v predlogu ponudnikom ter pristojnim pravosodnim ali drugim pooblaščenim neodvisnim upravnim organom otežuje predvidljivo in nesamovoljno uporabo zakonskih zahtev, ki jih uvaja predlog. EOVP in ENVP sta zaskrbljena, da bodo ti široki in nejasni pojmi povzročili pomanjkanje pravne varnosti in privedli tudi do precejšnjih razhajanj pri konkretnem izvajanju predloga po vsej Uniji, odvisno od razlag pojmov, kot so „verjetnost“ in „pretežno“, ki jih bodo podali pravosodni ali drugi neodvisni upravni organi v državah članicah. Tak izid ne bi bil sprejemljiv z vidika dejstva, da bodo določbe o odredbah o zaznavanju za ponudnike medosebnih komunikacijskih storitev pomenile „omejitve“ načela zaupnosti komunikacij, določenega v členu 5 direktive o zasebnosti in elektronskih komunikacijah, njihova jasnost in predvidljivost pa je zelo pomembna za zagotavljanje, da se te omejitve enotno uporabljajo po vsej Uniji.

4.5 Analiza potrebnosti in sorazmernosti predvidenih ukrepov³³

38. Kakor je navedeno zgoraj, obstajajo tri vrste odredb o zaznavanju, ki se lahko izdajo: odredbe o zaznavanju, ki se nanašajo na razširjanje znanih posnetkov spolne zlorabe otrok (člen 7(5) predloga), odredbe o zaznavanju, ki se nanašajo na razširjanje novih posnetkov spolne zlorabe otrok (člen 7(6) predloga), in odredbe o zaznavanju, ki se nanašajo na pridobivanje otrok za spolne namene (člen 7(7) predloga). Za vsako odredbo o zaznavanju bi običajno bila potrebna drugačna tehnologija za njeno praktično izvajanje. Posledično so stopnje njihove invazivnosti različne, zaradi česar je različen tudi vpliv na pravici do zasebnosti in varstva osebnih podatkov.
39. Tehnologije za zaznavanje znanih posnetkov spolne zlorabe otrok so običajno tehnologije, ki iščejo ujemanje, v smislu, da se opirajo na obstoječo zbirko podatkov o znanih posnetkih spolne zlorabe otrok, s katero lahko primerjajo slike (vključno z mirujočimi slikami iz videoposnetkov). Da se omogoči ujemanje, morajo biti slike, ki jih ponudnik obdeluje, in slike v podatkovni zbirki digitalizirane, kar se običajno zagotovi z njihovo pretvorbo v zgoščene vrednosti. Ocenjena stopnja lažno pozitivnih

(³³) Glej tudi The EDPS quick guide to necessity and proportionality (Kratki vodnik ENVP o potrebnosti in sorazmernosti), ki je na voljo na: https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

rezultatov pri taki zgoščevalni tehnologiji ne presega več kot 1 na 50 milijard (tj. 0,000000002-odstotna stopnja lažno pozitivnih rezultatov).³⁴

40. Za zaznavanje novih posnetkov spolne zlorabe otrok se običajno uporablja drugačna vrsta tehnologije, vključno s klasifikatorji in umetno inteligenco.³⁵ Stopnje napak so pri njih v splošnem precej višje. V Poročilu o oceni učinka je na primer navedeno, da obstajajo tehnologije za zaznavanje novih posnetkov spolne zlorabe otrok, katerih stopnja natančnosti se lahko nastavi na 99,9 odstotka (tj. 0,1-odstotno stopnjo lažno pozitivnih rezultatov), vendar lahko pri tej stopnji natančnosti prepoznajo le 80 odstotkov vseh posnetkov spolne zlorabe otrok v zadevnem podatkovnem naboru.³⁶
41. Kar zadeva zaznavanje pridobivanja otrok za spolne namene v komunikacijah, ki temeljijo na besedilu, je v Poročilu o oceni učinka pojasnjeno, da to običajno temelji na zaznavanju vzorcev. V omenjenem poročilu je navedeno, da je „stopnja točnosti“ pri nekaterih obstoječih tehnologijah za zaznavanje pridobivanja otrok za spolne namene 88-odstotna³⁷. Po navedbah Komisije to pomeni, da je „od 100 pogovorov, označenih kot morebitno kaznivo pridobivanje otrok za spolne namene, 12 takih, ki jih je mogoče na podlagi pregleda izključiti [v skladu s predlogom s strani Centra EU] in ki ne bodo naznanjeni organom kazenskega pregona“. ³⁸ Čeprav bi se predlog v nasprotju z začasno uredbo uporabljal tudi za zvočne komunikacije, pa Poročilo o oceni učinka ne obravnava tehnoloških rešitev, ki bi se lahko uporabljale za zaznavanje pridobivanja otrok za spolne namene v takem okolju.

4.5.1 Učinkovitost zaznavanja

42. Potrebnost pomeni potrebo po na dejstvih temelječi oceni učinkovitosti predvidenih ukrepov za doseganje postavljenega cilja in na dejstvih utemeljeni oceni, ali gre pri tem za manjše poseganje kot pri drugih možnostih za doseg istega cilja³⁹. Drug dejavnik, ki ga je treba upoštevati pri oceni sorazmernosti predlaganega ukrepa, je učinkovitost obstoječih ukrepov poleg predlaganega.⁴⁰ Če ukrepi za enak ali podoben namen že obstajajo, bi bilo treba njihovo učinkovitost oceniti v okviru ocene sorazmernosti. Brez take ocene učinkovitosti obstoječih ukrepov, ki imajo postavljen enak ali podoben namen, ni mogoče šteti, da je bil preizkus sorazmernosti novega ukrepa ustrezno opravljen.
43. Zaznavanje posnetkov spolne zlorabe otrok ali pridobivanja otrok za spolne namene s strani ponudnikov storitev gostovanja in medosebnih komunikacijskih storitev lahko pripomore k splošnemu cilju preprečevanja spolne zlorabe otrok in razširjanja posnetkov spolne zlorabe otrok po spletu ter

³⁴ Glej delovni dokument služb Komisije Poročilo o oceni učinka, spremni dokument k predlogu uredbe Evropskega parlamenta in Sveta o določitvi pravil za preprečevanje spolne zlorabe otrok in boj proti njej, SWD(2022) 209 final (v nadaljevanju: Poročilo o oceni učinka ali SWD(2022) 209 final), str. 281, op. 511.

³⁵ Poročilo o oceni učinka, str. 281.

³⁶ Prav tam, str. 282.

³⁷ Prav tam, str. 283.

³⁸ Predlog, COM(2022) 209 final, str. 14, op. 32.

³⁹ ENVP, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Tool kit (Ocenjevanje potrebnosti ukrepov, ki omejujejo temeljno pravico do varstva osebnih podatkov: zbirka orodij), 11. april 2017, str. 5; EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (Smernice ENVP za ocenjevanje sorazmernosti ukrepov, ki omejujejo temeljne pravice do zasebnosti in varstva osebnih podatkov), (19. december 2019), str. 8.

⁴⁰ ENVP, EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (Smernice ENVP za ocenjevanje sorazmernosti ukrepov, ki omejujejo temeljne pravice do zasebnosti in varstva osebnih podatkov) (19. december 2019), str. 11.

boja proti njima. Hkrati potreba po oceni učinkovitosti ukrepov, določenih v predlogu, sproža tri ključna vprašanja:

- Ali je mogoče ukrepe za zaznavanje spolne zlorabe otrok na spletu zlahka obiti?
- Kako bodo dejavnosti zaznavanja vplivale na ukrepanje organov kazenskega pregona?⁴¹
- Kako bi predlog zmanjšal pravno negotovost?

44. Podajanje podrobnih odgovorov na ta vprašanja ni naloga EOVP in ENVP. Kljub temu EOVP in ENVP opozarjata, da niti Poročilo o oceni učinka niti predlog teh vprašanj ne obravnavata v celoti.
45. Kar zadeva možnost izogibanja zaznavanju posnetkov spolne zlorabe otrok, je treba opozoriti, da se zdi, da tehnološke rešitve za zaznavanje posnetkov spolne zlorabe otrok, ki se izmenjujejo v šifrirani obliki, trenutno ni. Zato je mogoče vsako dejavnost zaznavanja – tudi pregledovanje na strani odjemalca, katerega namen je obiti šifriranje od konca do konca, ki ga ponuja ponudnik⁴² – zlahka obiti s šifriranjem vsebine z ločeno aplikacijo pred pošiljanjem vsebine ali njenim nalaganjem. Tako imajo lahko ukrepi za zaznavanje, predvideni s predlogom, manjši učinek na razširjanje posnetkov spolne zlorabe otrok po internetu, kot bi si morda želeli.
46. Poleg tega Komisija pričakuje, da se bo s sprejetjem obveznosti zaznavanja, ki jih uvaja predlog, povečalo število naznanitev spolne zlorabe otrok organom kazenskega pregona.⁴³ Kljub temu niti predlog niti Poročilo o oceni učinka ne pojasnjujeta, kako bo to odpravilo pomanjkljivosti sedanjega stanja. Glede na omejene vire organov kazenskega pregona se zdi, da je treba bolje razumeti, ali bi povečanje števila naznanitev imelo ustrezen učinek na dejavnosti organov kazenskega pregona zoper spolno zlorabo otrok. EOVP in ENVP želita v vsakem primeru poudariti, da bi bilo treba take naznanitve pravočasno oceniti, da se zagotovi čimprejšnje sprejetje odločitve o kazenskopravnem pomenu naznanjenih posnetkov in čim bolj omeji hramba nepomembnih podatkov.

4.5.2 Najmanj invaziven ukrep

47. Ob domnevi, da bi bili lahko uresničeni pozitivni učinki zaznavanja posnetkov spolne zlorabe otrok in pridobivanja otrok za spolne namene, ki ga je predvidela Komisija, mora biti zaznavanje najmanj invaziven ukrep glede na enako učinkovite ukrepe. Člen 4 predloga kot prvi korak določa, da bi morali ponudniki premisliti o sprejetju ukrepov za zmanjšanje tveganja za uporabo njihove storitve za spolno zlorabo otrok na spletu pod pragom, ki upravičuje izdajo odredbe o zaznavanju. Če obstajajo ukrepi za zmanjšanje tveganja, ki bi lahko privedli do znatnega zmanjšanja števila primerov pridobivanja otrok za spolne namene ali števila posnetkov spolne zlorabe otrok, ki se izmenjujejo v okviru zadevne storitve, bi ti ukrepi pogosto pomenili manj invazivne ukrepe v primerjavi z odredbo o zaznavanju⁴⁴. Zato bi morala, če zadevni ponudnik takih ukrepov ne sprejme prostovoljno, obstajati možnost, da pristojni neodvisni upravni organ ali pravosodni organ namesto izdaje odredbe o zaznavanju določi, da je izvajanje ukrepov za zmanjšanje tveganja obvezno in izvršljivo. Po mnenju EOVP in ENVP dejstvo, da člen 5(4) predloga usklajevalnemu organu omogoča, da od ponudnika „zahteva“, da uvede,

⁴¹ V Prilogi II k Poročilu o oceni učinka, str. 132, je navedeno, da je 85,71 odstotka anketirancev iz organov kazenskega pregona izrazilo zaskrbljenost zaradi povečanega števila posnetkov spolne zlorabe otrok v zadnjem desetletju in pomanjkanja virov (tj. kadrovskih in tehničnih).

⁴² Glej v nadaljevanju oddelek 4.10.

⁴³ Glej med drugim Prilogo 3 k Poročilu o oceni učinka, SWD(2022) 209 final, str. 176.

⁴⁴ Lahko bi bili na primer upoštevani ukrepi, kot je blokiranje prenosa posnetkov spolne zlorabe otrok na strani odjemalca s preprečevanjem nalaganja in pošiljanja vsebine elektronskih komunikacij, saj lahko ti ukrepi v nekaterih primerih pomagajo preprečiti kroženje znanih posnetkov spolne zlorabe otrok.

pregleda, odpravi ali razširi ukrepe za zmanjšanje tveganja, ni dovolj, saj taka zahteva ne bi bila neodvisno izvršljiva, njena neizpolnitev pa bi bila „kaznovana“ le z izdajo odredbe o zaznavanju.

48. Zato EOVP in ENVP menita, da bi moral biti usklajevalni organ ali pristojni neodvisni upravni ali pravosodni organ izrecno pooblaščen za naložitev manj invazivnih ukrepov za zmanjšanje tveganja pred izdajo odredbe o zaznavanju ali namesto take izdaje.

4.5.3 Sorazmernost v ozkem pomenu

49. Da bi ukrep spoštoval načelo sorazmernosti, določeno v členu 52(1) Listine, slabosti, ki jih ukrep povzroča v zvezi z uresničevanjem temeljnih pravic, ne bi smele prevladati nad prednostmi, ki izhajajo iz njega. Zato načelo sorazmernosti „omejuje organe pri izvrševanju pooblastil tako, da zahteva, da se uporabljena sredstva in postavljeni cilj (ali doseženi rezultat) uravnotežijo“.⁴⁵
50. Da se lahko oceni učinek ukrepa na temeljne pravice do zasebnosti in varstva osebnih podatkov, je zlasti pomembno natančno opredeliti:⁴⁶
- **področje uporabe ukrepa**, vključno s številom zadevnih oseb, in ali ukrep povzroča „postransko poseganje“ (tj. poseganje v zasebnost oseb, ki niso predmet ukrepa);
 - **obseg ukrepa**, vključno s količino zbranih informacij; trajanje; ali pregledovani ukrep zahteva zbiranje in obdelavo posebnih vrst podatkov;
 - **stopnjo invazivnosti** ob upoštevanju: narave dejavnosti, ki je predmet ukrepa (ali vpliva na dejavnosti, zajete z obveznostjo varovanja zaupnosti, odnos med odvetnikom in stranko; zdravstvena dejavnost); ali ustreza oblikovanju profilov zadevnih posameznikov; ali obdelava vključuje (delno ali popolno) uporabo sistema avtomatiziranega sprejemanja odločitev z „območjem napake“;
 - ali se ukrep nanaša na **ranljive osebe**;
 - ali vpliva tudi na **druge temeljne pravice** (na primer pravico do svobode izražanja, kakor v zadevah *Digital Rights Ireland* in *Seitlinger* in drugi ter *Tele2 Sverige* in *Watson*).⁴⁷

⁴⁵ Glej sodbo Sodišča z dne 8. julija 2010, *Afton Chemical*, C-343/09, točka 45; sodbo Sodišča z dne 9. novembra 2010, *Volker und Markus Schecke in Hartmut Eifert*, združeni zadevi C-92/09 in C-93/09, točka 74; sodbo Sodišča z dne 23. oktobra 2012, *Nelson in drugi*, združeni zadevi C-581/10 in C-629/10, točka 71; sodbo Sodišča z dne 22. januarja 2013, *Sky Österreich*, C-283/11, točka 50; in sodbo Sodišča z dne 17. oktobra 2013, *Schaible*, C-101/12, točka 29. Glej še Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit (Ocenjevanje potrebnosti ukrepov, ki omejujejo temeljno pravico do varstva osebnih podatkov: zbirka orodij) (11. april 2017).

⁴⁶ ENVP, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (Smernice za ocenjevanje sorazmernosti ukrepov, ki omejujejo temeljne pravice do zasebnosti in varstva osebnih podatkov) (19. december 2019), str. 23.

⁴⁷ Glej tudi Mnenje 7/2020 Evropskega nadzornika za varstvo podatkov o predlogu za začasna odstopanja od Direktive 2002/58/ES za namene boja proti spolni zlorabi otrok na spletu (10. november 2020), str. 9 in naslednje.

51. V tem okviru je tudi pomembno opozoriti, da je učinek v zvezi z zadevnim posameznikom lahko sicer majhen, vendar še vedno velik ali zelo velik za skupnost oziroma družbo kot celoto.⁴⁸
52. Pri vseh treh vrstah odredb o zaznavanju (zaznavanje znanih posnetkov spolne zlorabe otrok, novih posnetkov spolne zlorabe otrok in pridobivanja otrok za spolne namene) se tehnologije, ki so trenutno na voljo, opirajo na avtomatizirano obdelavo vsebinskih podatkov vseh zadevnih uporabnikov. Tehnologije, ki se uporabljajo za analizo vsebine, so pogosto zapletene in običajno vključujejo uporabo umetne inteligence. Posledično delovanje te tehnologije uporabniku storitve morda ni popolnoma razumljivo. Poleg tega je znano, da so stopnje napak pri tehnologijah, ki so trenutno na voljo, zlasti tistih za zaznavanje novih posnetkov spolne zlorabe otrok ali pridobivanja otrok za spolne namene, razmeroma visoke.⁴⁹ Obstaja tudi tveganje za naznanitev Centru EU v skladu s členoma 12(1) in 48(1) predloga na podlagi zaznavanja „potencialnih“ posnetkov spolne zlorabe otrok.
53. Poleg tega lahko splošni pogoji za izdajo odredbe o zaznavanju v skladu s predlogom, tj. uporabljeni za celotno storitev in ne le za izbrane komunikacije⁵⁰, do 24-mesečno trajanje odredbe za znane ali nove posnetke spolne zlorabe otrok ter do 12-mesečno trajanje odredbe v zvezi s pridobivanjem otrok za spolne namene⁵¹ itd., privedejo do zelo širokega področja uporabe odredbe v praksi. Posledično bi bilo spremljanje po svoji naravi dejansko splošno in neselektivno, v praksi pa ne bi bilo usmerjeno.
54. Glede na navedeno sta EOVP in ENVP zaskrbljena tudi glede mogočih zastraševalnih učinkov v zvezi z uresničevanjem svobode izražanja. EOVP in ENVP opozarjata, da se zdi, da manjša kot je jasnost zakona, verjetnejši je tak zastraševalni učinek.
55. Ker ni specifičnosti, natančne opredeljenosti in jasnosti, ki so potrebne za izpolnitev zahteve glede pravne varnosti,⁵² in glede na široko področje uporabe predloga, tj. uporablja se za vse ponudnike ustreznih storitev informacijske družbe, ki ponujajo take storitve v Uniji,⁵³ predlog ne zagotavlja, da bo dejansko vzpostavljen le ciljno usmerjen pristop k zaznavanju posnetkov spolne zlorabe otrok in pridobivanja otrok za spolne namene. EOVP in ENVP zato menita, da bi predlog v praksi lahko postal podlaga za dejansko splošno in neselektivno pregledovanje vsebin skoraj vseh vrst elektronskih komunikacij vseh uporabnikov v EU/EGP. Posledično lahko zakonodaja ljudi spodbudi k temu, da se vzdržijo izmenjave zakonitih vsebin zaradi strahu, da bi bili lahko na podlagi svojega ravnanja tarča takega pregleda.
56. EOVP in ENVP priznavata, da lahko različni ukrepi za boj proti spolni zlorabi otrok na spletu zajemajo različne stopnje invazivnosti. EOVP in ENVP najprej ugotavljata, da avtomatizirana analiza govora ali besedila zaradi odkrivanja morebitnih primerov pridobivanja otrok za spolne namene verjetno pomeni hujše poseganje kot iskanje ujemanja slik ali videoposnetkov na podlagi predhodno potrjenih primerov posnetkov spolne zlorabe otrok zaradi zaznavanja njihovega razširjanja. Poleg tega je treba razlikovati med zaznavanjem „znanih posnetkov spolne zlorabe otrok“ in „novih posnetkov spolne zlorabe otrok“.

⁴⁸ ENVP, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (Smernice za ocenjevanje sorazmernosti ukrepov, ki omejujejo temeljne pravice do zasebnosti in varstva osebnih podatkov) (19. december 2019), str. 20.

⁴⁹ Za podrobnosti glej oddelek 4.5 zgoraj in pododdelek v nadaljevanju 4.8.2.

⁵⁰ Glej člen 7(1) predloga.

⁵¹ Glej tretji pododstavek člena 7(9) predloga.

⁵² Glej sodbo Sodišča z dne 13. marca 1997, *Komisija Evropskih skupnosti proti Francoski republiki*, C-197/96, točka 15.

⁵³ Glej člen 1(2) predloga.

Dodatno je treba razlikovati učinek med ukrepi, naslovljenimi na ponudnike storitev gostovanja, in tistimi, naloženimi ponudnikom medosebnih komunikacijskih storitev.

4.5.4 Zaznavanje znanih posnetkov spolne zlorabe otrok

57. Čeprav bi bil predlog v skladu z uvodno izjavo 4 „tehnološko nevtralen“, bosta učinkovitost predlaganih ukrepov za zaznavanje in njihov učinek na posameznike močno odvisna od izbire uporabljene tehnologije in izbranih kazalnikov. Tega dejstva se zaveda tudi Komisija v Prilogi 8 k Poročilu o oceni učinka⁵⁴, potrjujejo pa ga tudi druge študije, kot je ciljno usmerjena nadomestna ocena učinka predloga Komisije o začasnem odstopanju od direktive o zasebnosti in elektronskih komunikacijah za namene boja proti spolni zlorabi otrok na spletu, ki jo je februarja 2021 opravila Služba Evropskega parlamenta za raziskave.⁵⁵
58. Člen 10 predloga določa več zahtev za tehnologije, ki se uporabljajo za zaznavanje, zlasti glede njihove učinkovitosti, zanesljivosti in najmanjše invazivnosti v smislu vpliva na pravice uporabnikov do zasebnega in družinskega življenja, vključno z zaupnostjo komunikacij, in do varstva osebnih podatkov uporabnikov.
59. V tem okviru EOVP in ENVP opozarjata, da so trenutno edine tehnologije, za katere se zdi, da lahko v splošnem izpolnjujejo te standarde, tiste, ki se uporabljajo za zaznavanje znanih posnetkov spolne zlorabe otrok, tj. tehnologije, ki iščejo ujemanje, pri tem pa se opirajo na zbirko podatkov o zgoščenih vrednostih kot referenčno točko.

4.5.5 Zaznavanje predhodno neznanih posnetkov spolne zlorabe otrok

60. Iz ocene ukrepov, namenjenih zaznavanju predhodno neznanih (novih) posnetkov spolne zlorabe otrok, izhajajo različne ugotovitve glede njihove učinkovitosti, zanesljivosti in omejevanja vpliva na temeljne pravice do zasebnosti in varstva podatkov.
61. Prvič, kakor je pojasnjeno v Poročilu o oceni učinka k predlogu, tehnologije, ki se trenutno uporabljajo za zaznavanje predhodno neznanih posnetkov spolne zlorabe otrok, vključujejo klasifikatorje in umetno inteligenco. Klasifikator je vsak algoritem, ki z zaznavanjem vzorca razvršča podatke v označene razrede ali skupine informacij.⁵⁶ Tako dajejo te tehnologije različne rezultate in imajo različen učinek v smislu točnosti, učinkovitosti in stopnje invazivnosti. Hkrati so tudi dovzetnejše za napake.
62. Tehnike, ki se uporabljajo za zaznavanje predhodno neznanih posnetkov spolne zlorabe otrok, so podobne tistim, ki se uporabljajo za zaznavanje pridobivanja otrok za spolne namene, saj oboje temeljijo na modelih za napovedovanje, ki uporabljajo tehnologije umetne inteligence, ne pa na preprostih tehnologijah iskanja ujemanja. EOVP in ENVP menita, da je potrebna zelo velika previdnost pri zaznavanju predhodno neznanih posnetkov spolne zlorabe otrok, saj bi napaka sistema povzročila

⁵⁴ Glej informacije o stopnjah lažno pozitivnih rezultatov v Prilogi 8 k Poročilu o oceni učinka, str. 279 in naslednje.

⁵⁵ Glej Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse: Targeted substitute impact assessment (Predlog Komisije o začasnem odstopanju od direktive o zasebnosti in elektronskih komunikacijah za namene boja proti spolni zlorabi otrok na spletu: ciljno usmerjena nadomestna ocena učinka) (Služba Evropskega parlamenta za raziskave, februar 2021), str. 14 in naslednje.

⁵⁶ Priloga 8 k Poročilu o oceni učinka, str. 281.

hude posledice za posameznike, na katere se nanašajo osebni podatki, ki bi bili samodejno označeni kot morebitni storilci zelo hudega kaznivega dejanja, njihovi osebni podatki in podrobnosti njihovih komunikacij pa bi bili naznanjeni.

63. Drugič, kazalniki smotrnosti v literaturi (nekateri so poudarjeni v spremnem Poročilu o oceni učinka k predlogu)⁵⁷ prinašajo zelo malo informacij o pogojih, uporabljenih za njihov izračun, in njihovem ustrežanju resničnim življenjskim razmeram, kar pomeni, da bi bila lahko smotrnost v resničnem svetu znatno manjša od pričakovane, zaradi česar bi bila točnost manjša, odstotek „lažno pozitivnih rezultatov“ pa višji.
64. Tretjič, kazalnike smotrnosti bi bilo treba obravnavati v konkretnih okoliščinah uporabe zadevnih orodij za zaznavanje, poleg tega pa bi ti kazalniki morali zagotoviti izčrpen vpogled v delovanje orodij za zaznavanje. Glede uporabe algoritmov umetne inteligence v zvezi s slikami ali besedilom je dobro dokumentirano, da lahko zaradi pomanjkljive zastopanosti nekaterih skupin prebivalstva v podatkih, uporabljenih za urjenje algoritma, pride do pristranskosti in diskriminacije. Te pristranskosti je treba opredeliti, izmeriti in zmanjšati na sprejemljivo raven, da bodo sistemi za zaznavanje resnično koristni za družbo kot celoto.
65. Čeprav je bila opravljena študija tehnologij za zaznavanje,⁵⁸ EOVP in ENVP menita, da je za oceno zanesljivosti obstoječih orodij potrebna nadaljnja analiza. Ta analiza bi morala temeljiti na izčrpnih kazalnikih smotrnosti, oceniti pa bi morala učinek morebitnih napak v resničnih življenjskih razmerah za vse posameznike, na katere se nanašajo osebni podatki in predlog.
66. Kakor je navedeno zgoraj, EOVP in ENVP resno dvomita glede zadostnosti obsega postopkovnih zaščitnih ukrepov iz člena 7(6) predloga za zmanjšanje teh tveganj. Poleg tega, kakor je navedeno zgoraj, opozarjata, da predlog za opisovanje sprejemljive količine tveganja uporablja precej abstraktne in nejasne pojme (na primer „pretežno“).
67. EOVP in ENVP sta zaskrbljena, da bodo ti široki in nejasni pojmi povzročili pomanjkanje pravne varnosti in izvali tudi močna razhajanja pri konkretnem izvajanju predloga po vsej Uniji, odvisno od razlag pojmov, kot so „verjetnost“ in „pretežno“, ki jih bodo podali pravosodni ali drugi neodvisni upravni organi v državah članicah. To je skrb vzbujajoče tudi z vidika dejstva, da bodo določbe o odredbah o zaznavanju pomenile „omejitve“ načela zaupnosti, določenega v členu 5 direktive o zasebnosti in elektronskih komunikacijah. Zato je treba v predlagani uredbi izboljšati njihovo jasnost in predvidljivost.

4.5.6 Zaznavanje pridobivanja otrok za spolne namene

68. EOVP in ENVP ugotavljata, da predlagani ukrepi, ki se nanašajo na zaznavanje pridobivanja otrok za spolne namene, ki vključuje avtomatizirano analizo govora ali besedila, verjetno pomenijo najhujše poseganje v pravice uporabnikov do zasebnega in družinskega življenja, vključno z zaupnostjo komunikacij, in do varstva osebnih podatkov uporabnikov.
69. Čeprav je mogoče področje uporabe zaznavanja znanih in celo novih posnetkov spolne zlorabe otrok omejiti na analizo slik in videoposnetkov, bi se zaznavanje pridobivanja otrok za spolne namene po svoji naravi razširilo na vse komunikacije, ki temeljijo na besedilu (in mogoče zvočne komunikacije) in

⁵⁷ Priloga 8 k Poročilu o oceni učinka, str. 281–283.

⁵⁸ Poročilo o oceni učinka, str. 279 in naslednje.

ki spadajo na področje uporabe odredbe o zaznavanju. Posledično je intenzivnost zadevnega poseganja v zaupnost komunikacij precej večja.

70. EOVP in ENVP menita, da dejanska splošna in neselektivna avtomatizirana analiza komunikacij, ki temeljijo na besedilu in se prenašajo prek medosebnih komunikacijskih storitev, z vidika odkrivanja morebitnega pridobivanja otrok za spolne namene ne izpolnjuje zahtev glede potrebnosti in sorazmernosti. Tudi če se uporabljena tehnologija omeji na uporabo kazalnikov, EOVP in ENVP menita, da je uporaba take splošne in neselektivne analize pretirana in lahko celo vpliva na samo bistvo temeljne pravice do zasebnosti, določene v členu 7 Listine.
71. Kakor je bilo že navedeno, pomanjkanja vsebinskih zaščitnih ukrepov v okviru ukrepov za zaznavanje pridobivanja otrok za spolne namene ni mogoče nadomestiti zgolj s postopkovnimi zaščitnimi ukrepi. Poleg tega je težava s pomanjkanjem zadostne pravne jasnosti in varnosti (na primer uporaba nejasnega pravnega jezika, kot je „pretežno“) še hujša pri avtomatizirani analizi osebnih komunikacij, ki temeljijo na besedilu, v primerjavi s primerjanjem fotografij na podlagi zgoščevalne tehnologije.
72. EOVP in ENVP še menita, da je „zastraševalni učinek“ na svobodo izražanja še posebej velik, kadar se besedilne (ali zvočne) komunikacije posameznikov obsežno pregledujejo in analizirajo. EOVP in ENVP opozarjata, da manjša kot je jasnost zakona, hujši je tak zastraševalni učinek.
73. Poleg tega je, kakor je navedeno v Poročilu o oceni učinka⁵⁹ in študiji Službe Evropskega parlamenta za raziskave⁶⁰, stopnja točnosti tehnologij za zaznavanje pridobivanja otrok za spolne namene na podlagi besedila veliko nižja od stopnje točnosti tehnologij za zaznavanje znanih posnetkov spolne zlorabe otrok⁶¹. Tehnike zaznavanja pridobivanja otrok za spolne namene so zasnovane za analizo in določitev verjetnostnih ocen za vsak vidik pogovora, zaradi česar EOVP in ENVP tudi menita, da so dovzetne za napake in zlorabo.

4.5.7 Ugotovitev o potrebnosti in sorazmernosti predvidenih ukrepov

74. Kar zadeva potrebnost in sorazmernost predvidenih ukrepov za zaznavanje, sta EOVP in ENVP zlasti zaskrbljena glede ukrepov, predvidenih za zaznavanje neznanih posnetkov spolne zlorabe otrok in pridobivanja otrok za spolne namene, zaradi njihove invazivnosti, morebitne odobritve splošnega dostopa do vsebin komunikacij, verjetnostne narave teh ukrepov in stopenj napak, povezanih s takimi tehnologijami.
75. Poleg tega je na podlagi sodne prakse Sodišča mogoče sklepati, da je verjetneje, da bodo ukrepi, ki javnim organom dovoljujejo splošen dostop do vsebine komunikacije, vplivali na bistveno vsebino pravic, zajamčenih v členih 7 in 8 Listine. Ti premisleki so posebej pomembni v zvezi z ukrepi za zaznavanje pridobivanja otrok za spolne namene, predvidenimi s predlogom.
76. EOVP in ENVP v vsakem primeru menita, da poseganje, ustvarjeno zlasti z ukrepi za zaznavanje pridobivanja otrok za spolne namene, presega, kar je nujno potrebno in sorazmerno. Te ukrepe bi bilo zato treba odstraniti iz predloga.

⁵⁹ Priloga 8 k Poročilu o oceni učinka, str. 281–283.

⁶⁰ Str. 15–18.

⁶¹ Glej zgoraj, točka (40).

4.6 Obveznosti naznanitve

77. EOVP in ENVP priporočata dopolnitev seznama specifičnih zahtev za naznanjanje v členu 13 predloga z zahtevo, da se v naznanitev vključijo informacije o konkretni tehnologiji, ki je ponudniku omogočila, da izve za zadevno neprimerno vsebino, če je ponudnik izvedel za morebitno spolno zlorabo otrok po ukrepih, sprejetih za izvršitev odredbe o zaznavanju, izdane v skladu s členom 7 predloga.

4.7 Obveznosti odstranitve in blokiranja dostopa

78. Eden od ukrepov, predvidenih s predlogom, za zmanjšanje tveganj za razširjanje posnetkov spolne zlorabe otrok je izdaja odredb o odstranitvi in blokiranju dostopa, ki bi ponudnike zavezale k odstranitvi posnetkov spolne zlorabe otrok ali onemogočitvi ali blokiranju dostopa do njih.⁶²
79. Čeprav je vpliv odredb o odstranitvi na varstvo podatkov in zasebnost komunikacij razmeroma omejen, EOVP in ENVP s splošno pripombo opozarjata, da mora biti upoštevano splošno načelo, da bi vsak tak ukrep moral biti čim bolj ciljno usmerjen.
80. EOVP in ENVP hkrati opozarjata na dejstvo, da imajo ponudniki storitev dostopa do interneta dostop do konkretnega URL vsebine le, če je vsebina na voljo v golem besedilu. Če je dostop do vsebine omogočen prek HTTPS, ponudnik storitev dostopa do interneta ne bo imel dostopa do konkretnega URL, razen če komunikacijo dešifrira. Zato EOVP in ENVP dvomita v učinkovitost ukrepov za blokiranje dostopa ter menita, da bi bila zahteva, da ponudniki storitev dostopa do interneta dešifrirajo spletne komunikacije, da se lahko blokira dostop do tistih, ki se nanašajo na posnetke spolne zlorabe otrok, nesorazmerna.
81. Splošneje je treba še opozoriti, da je blokiranje (ali onemogočitev) dostopa do digitalnega elementa postopek, ki poteka na ravni omrežja, njegova izvedba pa se lahko izkaže za neuspešno, kadar obstaja več (morda podobnih in ne enakih) kopij istega elementa. Poleg tega se lahko tak postopek izkaže za nesorazmernega, če blokiranje dostopa vpliva na druge digitalne elemente, ki niso nezakoniti, kadar so ti shranjeni v istem strežniku, do katerega se dostop prekine z uporabo omrežnih ukazov (na primer z uvrstitvijo IP-naslova na črni seznam ali uvrstitvijo na črni seznam na podlagi DNS). Poleg tega niso vsi pristopi k blokiranju dostopa na omrežni ravni enako uspešni, nekatere pa je mogoče zlahka obiti z dokaj osnovnimi tehničnimi veščinami.
82. Nazadnje bi bilo treba v predlagani uredbi pojasniti pooblastila usklajevalnih organov glede izdaje odredb o blokiranju dostopa. Iz sedanjega besedila členov 16(1) in 17(1) denimo ni jasno, ali so usklajevalni organi pooblaščen za izdajo ali le za zahtevanje izdaje odredb o blokiranju dostopa.⁶³

⁶²)Člena 14 in 16 predloga.

⁶³ Člen 16(1) predloga se glasi: „Usklajevalni organ v državi sedeža je pooblaščen, da od pristojnega pravosodnega organa države članice, ki ga je imenovala, ali od neodvisnega upravnega organa te države članice zahteva, naj izda odredbo o blokiranju dostopa [...]“, člen 17(1) pa se glasi: „Usklajevalni organ v državi sedeža izda odredbe o blokiranju dostopa iz člena 16 [...]“ (poudarek dodan).

4.8 Ustrezne tehnologije in zaščitni ukrepi

4.8.1 Vgrajeno in privzeto varstvo podatkov

83. Zdi se, da zahteve predloga, ki se uporabljajo za tehnologije za zaznavanje posnetkov spolne zlorabe otrok in pridobivanja otrok za spolne namene, niso dovolj stroge. EOVP in ENVP zlasti opozarjata, da predlog v nasprotju s podobnimi določbami začasne uredbe⁶⁴ ne omenja izrecno načela vgrajenega in privzetega varstva podatkov in ne določa, da tehnologije, ki se uporabljajo za pregledovanje besedila v komunikacijah, ne smejo biti zmožne razbrati vsebine komunikacij. Predlog v členu 10(3)(b) zgolj določa, da morajo biti tehnologije take, da iz ustreznih komunikacij ne morejo „izluščiti“ nobenih drugih informacij, razen tistih, ki so nujne za zaznavanje. Kljub temu se zdi, da ta standard ni dovolj strog, saj bi bilo mogoče brez *izluščenja* informacij iz vsebine komunikacije kot take *razbrati* druge informacije.
84. Posledično EOVP in ENVP priporočata, da se v predlog vnese uvodna izjava, ki določa, da se za tehnologije, ki jih ureja člen 10 predloga, načelo vgrajenega in privzetega varstva podatkov, določeno v členu 25 Uredbe (EU) 2016/679, uporablja na podlagi zakona, zaradi česar ga v pravnem besedilu ni treba ponoviti. Pravtako bi bilo treba spremeniti člen 10(3)(b), da se poleg tega, da druge informacije ne morejo biti izluščene, zagotovi tudi, da ne morejo biti razbrane, kakor je trenutno določeno v členu 3(1)(b) začasne uredbe.

4.8.2 Zanesljivost tehnologij

85. Predlog domneva, da bi ponudniki storitev za izvrševanje odredb o zaznavanju lahko uporabili različne vrste tehnoloških rešitev. Predlog zlasti domneva, da so sistemi umetne inteligence za zaznavanje neznanih posnetkov spolne zlorabe otrok in zaznavanja pridobivanja otrok za spolne namene na voljo in da delujejo⁶⁵ ter da bi jih nekateri usklajevalni organi lahko obravnavali kot najsodobnejše. Čeprav se učinkovitost predloga opira na zanesljivost teh tehnoloških rešitev, je o splošni in sistematični uporabi teh tehnik na voljo zelo malo informacij, zaradi česar je skrben premislek upravičen.
86. Čeprav sta EOVP in ENVP v oceni sorazmernosti zaradi pomanjkanja alternativ morala uporabiti kazalnike smotrnosti tehnologij zaznavanja, navedene v spremnem Poročilu o oceni učinkovitosti k predlogu, je treba še opozoriti, da je glede teh kazalnikov navedenih zelo malo informacij o tem, kako so bili ocenjeni, in o tem, ali izražajo smotrnost zadevnih tehnologij v resničnem svetu. Ni informacij o preizkusih ali referenčnih merilih, ki jih dobavitelji tehnologij uporabljajo za merjenje te smotrnosti. Brez takih informacij preizkusov ni mogoče ponoviti ali oceniti veljavnosti izjav glede smotrnosti. Glede tega je treba opozoriti, da čeprav bi se lahko kazalniki smotrnosti razlagali tako, da je stopnja točnosti nekaterih orodij zelo visoka (na primer točnost nekaterih orodij za zaznavanje pridobivanja otrok za spolne namene je 88-odstotna),⁶⁶ bi morali biti ti kazalniki obravnavani z vidika predvidene praktične uporabe orodij za zaznavanje in resnosti tveganj, ki bi jih nepravilna ocena zadevnih posnetkov pomenila za zadevne posameznike, na katere se nanašajo osebni podatki. Poleg tega EOVP in ENVP menita, da je pri taki visokotvegani obdelavi 12-odstotna stopnja neuspeha veliko tveganje za posameznike, na katere se nanašajo osebni podatki in za katere so dobljeni lažno pozitivni rezultati, tudi če obstajajo zaščitni ukrepi za preprečevanje lažnih naznanitev organom kazenskega pregona.

⁽⁶⁴⁾ Člen 3(1)(b) začasne uredbe.

⁶⁵ Glej Poročilo o oceni učinka, str. 281–282.

⁶⁶ Prav tam, str. 283.

Zelo malo je verjetno, da bi ponudniki storitev za pregled takega odstotka lažno pozitivnih rezultatov namenili dovolj virov.

87. Kakor je bilo navedeno,⁶⁷ bi kazalniki smotrnosti morali zagotoviti izčrpen vpogled v delovanje orodij za zaznavanje. Glede uporabe algoritmov umetne inteligence v zvezi s slikami ali besedilom je dobro dokumentirano, da lahko zaradi pomanjkljive zastopanosti nekaterih skupin prebivalstva v podatkih, uporabljenih za urjenje algoritma, pride do pristranskosti in diskriminacije. Te pristranskosti je treba opredeliti, izmeriti in zmanjšati na sprejemljivo raven, da bodo sistemi za zaznavanje družbi kot celoti prinesli resnične koristi.
88. Čeprav je bila opravljena študija tehnologij za zaznavanje,⁶⁸ EOVP in ENVP menita, da je za neodvisno oceno zanesljivosti uporabe obstoječih orodij v primerih iz resničnega sveta potrebna nadaljnja analiza. Ta analiza bi morala temeljiti na izčrpnih kazalnikih smotrnosti, oceniti pa bi morala učinek morebitnih napak v resničnih življenjskih razmerah za vse posameznike iz predloga, na katere se nanašajo osebni podatki. Ker so te tehnologije podlaga, na katero se opira predlog, EOVP in ENVP menita, da je ta analiza izjemno pomembna za oceno ustreznosti predloga.
89. EOVP in ENVP še opozarjata, da predlog ne opredeljuje tehnološko specifičnih zahtev, ne glede na to, ali gre za stopnje napak, uporabo klasifikatorjev in njihovo potrjevanje ali druge omejitve. Tako je prepuščeno praksi, da taka merila oblikuje pri oceni sorazmernosti uporabe konkretne tehnologije, kar dodatno pripomore k pomanjkanju natančnosti in jasnosti.
90. Glede na pomembnost posledic lažno pozitivnih rezultatov za posameznike, na katere se nanašajo osebni podatki, EOVP in ENVP menita, da bi bilo treba stopnje lažno pozitivnih rezultatov čim bolj zmanjšati in da morajo biti navedeni sistemi zasnovani ob upoštevanju, da velika večina elektronskih komunikacij ne vključuje niti posnetkov spolne zlorabe otrok niti pridobivanja otrok za spolne namene in da bo glede na količino podatkov, ki bodo predmet zaznavanja, celo zelo nizka stopnja lažno pozitivnih rezultatov pomenila zelo veliko število lažno pozitivnih rezultatov. Splošneje, EOVP in ENVP sta tudi zaskrbljena zaradi dejstva, da smotrnost razpoložljivih orodij, navedenih v Poročilu o oceni učinka, ne izraža natančnih in primerljivih kazalnikov glede stopenj lažno pozitivnih in lažno negativnih rezultatov, ter menita, da bi bilo treba izdati primerljive in ustrezne kazalnike smotrnosti za navedene tehnologije, preden bi se jih štelo za razpoložljive in učinkovite.

4.8.3 Pregledovanje zvočnih komunikacij

91. V nasprotju z začasno uredbo⁶⁹ predlog ne izključuje iz svojega področja uporabe pregledovanja zvočnih komunikacij v okviru zaznavanja pridobivanja otrok za spolne namene.⁷⁰ EOVP in ENVP menita, da je pregledovanje zvočnih komunikacij še posebej invazivno, saj bi običajno zahtevalo aktivno in stalno prestrezanje „v živo“. Poleg tega je zasebnost izgovorjene besede v nekaterih državah članicah posebej varovana.⁷¹ Prav tako je zaradi dejstva, da bi bilo treba načeloma analizirati vso vsebino zvočne komunikacije, verjetno, da bo ta ukrep vplival na bistveno vsebino pravic, zajamčenih v členih 7 in 8 Listine. Ta način zaznavanja bi zato moral ostati zunaj področja obveznosti zaznavanja, določenih v predlagani uredbi, tako v zvezi z glasovnimi sporočili kot tudi komunikacijami v živo, še

⁶⁷ Glej točki 63 in 64 zgoraj.

⁶⁸ Glej Poročilo o oceni učinka, str. 279 in naslednje.

⁶⁹ Glej člen 1(2) začasne uredbe.

⁷⁰ Glej člen 1 predloga.

⁷¹ Glej na primer člen 201 nemškega kazenskega zakonika.

zlasti z vidika dejstva, da v spremnem Poročilu o oceni učinka k predlogu niso opredeljena konkretna tveganja ali spremembe na področju groženj, ki bi upravičila njegovo uporabo.⁷²

4.8.4 Preverjanje starosti

92. Predlog ponudnike spodbuja, da za prepoznavanje otroških uporabnikov svojih storitev uporabljajo ukrepe za preverjanje starosti in oceno starosti.⁷³ Glede tega EOVP in ENVP opozarjata, da trenutno ni tehnološke rešitve, ki bi lahko v spletnem okolju zanesljivo ocenila starost uporabnika, ne da bi se opirala na uradno digitalno identiteto, ki pa v tej fazi ni na voljo vsem evropskim državljanom.⁷⁴ Zato bi s predlogom predvidena uporaba ukrepov za preverjanje starosti lahko mogoče privedla do tega, da bi bile na primer odrasle osebe mladega videza izključene iz dostopa do spletnih storitev ali da bi se uporabljala zelo invazivna orodja za preverjanje starosti, ki bi lahko zavirala zakonito uporabo zadevnih storitev ali odvrčala od take uporabe.
93. V zvezi s tem, čeprav so v uvodni izjavi 16 predloga kot mogoči ukrepi za zmanjšanje tveganja omenjena orodja za starševski nadzor, EOVP in ENVP priporočata, da se predlagana uredba spremeni tako, da ponudnikom izrecno dovoli, da se poleg preverjanja starosti ali namesto njega opirajo na mehanizme starševskega nadzora.

4.9 Ohranjanje informacij

94. Člen 22 omejuje namene, za katere lahko ponudniki, za katere velja predlog, hranijo podatke o vsebini in druge podatke, ki se obdelujejo v zvezi z ukrepi, sprejetimi za zagotavljanje izpolnjevanja obveznosti, določenih v predlogu. Kljub temu je v predlogu navedeno, da lahko ponudniki te informacije hranijo tudi za izboljšanje učinkovitosti in natančnosti tehnologij za zaznavanje spolne zlorabe otrok na spletu za izvršitev odredbe o zaznavanju, vendar v ta namen ne smejo hraniti nobenih osebnih podatkov.⁷⁵
95. EOVP in ENVP menita, da bi bilo treba hrambo podatkov za izboljšanje učinkovitosti in natančnosti tehnologij dovoliti le tistim ponudnikom, ki uporabljajo lastne tehnologije za zaznavanje, tisti, ki pa uporabljajo tehnologije, ki jih zagotovi Center EU, pa te možnosti ne bi smeli imeti. Poleg tega EOVP in ENVP opozarjata, da bo v praksi morda težko poskrbeti, da se nobeni osebni podatki ne bodo hranili za navedeni namen, saj je verjetno, da bo večina podatkov o vsebini in drugih podatkov, ki se obdelujejo za namen zaznavanja, opredeljena kot osebni podatki.

4.10 Vpliv na šifriranje

96. Evropski organi za varstvo podatkov dosledno zagovarjajo široko razširjeno razpoložljivost orodij za močno šifriranje in nasprotujejo kakršnim koli stranskim vratom.⁷⁶ To je zato, ker je šifriranje pomembno za zagotovitev uživanja vseh človekovih pravic na spletu in zunaj njega.⁷⁷ Poleg tega tehnologije šifriranja bistveno pripomorejo tako k spoštovanju zasebnega življenja in zaupnosti

⁷² Glej Poročilo o oceni učinka.

⁷³ Glej člen 4(3) in člen 6(1)(c) ter uvodno izjavo 16 predloga.

⁷⁴ Glej na primer francosko nacionalno komisijo za informatiko in svoboščine CNIL, Priporočilo 7: Preverite starost otroka in starševsko privolitve ob spoštovanju otrokove zasebnosti (9. avgust 2021).

⁷⁵ Člen 22(1) predloga.

⁷⁶ Glej na primer Izjavo Delovne skupine za varstvo podatkov iz člena 29 o šifriranju in njegovem vplivu na varstvo posameznikov pri obdelavi njihovih osebnih podatkov v EU (11. april 2018).

⁷⁷ Glej Resolucijo 47/16 Sveta za človekove pravice o spodbujanju, varstvu in uživanju človekovih pravic na internetu, dokument ZNA/HRC/RES/47/16 (26. julij 2021).

komunikacij kot tudi k inovacijam in rasti digitalnega gospodarstva, ki se opira na visoko raven zaupanja in zanesljivosti, ki jo zagotavljajo take tehnologije.

97. Šifriranje od konca do konca je v okviru medosebnih komunikacij ključno orodje za zagotavljanje zaupnosti elektronskih komunikacij, saj zagotavlja močne tehnične zaščitne ukrepe zoper dostop katerih koli oseb, vključno s ponudnikom, razen pošiljatelja in prejemnika(-ov), do vsebine komunikacij. Preprečevanje uporabe šifriranja od konca do konca ali kakršno koli odvrčanje od nje, nalaganje ponudnikom storitev obveznosti, da podatke iz elektronskih komunikacij obdelujejo za namene, ki se ne nanašajo na zagotavljanje njihovih storitev, ali nalaganje ponudnikom obveznosti, da tretjim osebam proaktivno posredujejo elektronske komunikacije, bi pomenilo tveganje, da bi ponudniki ponujali manj šifrirane storitve, da bi bolje izpolnjevali obveznosti, kar bi oslabilo vlogo šifriranja na splošno in ogrozilo spoštovanje temeljnih pravic evropskih državljanov. Čeprav je šifriranje od konca do konca eden od najpogostejše uporabljenih varnostnih ukrepov v okviru elektronskih komunikacij, je treba opozoriti, da so druge tehnične rešitve (na primer uporaba drugih kriptografskih shem) lahko enako pomembne ali bi lahko postale enako pomembne za varstvo in zaščito zaupnosti digitalnih komunikacij. Zato se tudi njihove uporabe ne bi smelo preprečevati ali odvrčati od nje.
98. Uporaba orodij za prestrezanje in analizo medosebnih elektronskih komunikacij je pravzaprav v nasprotju s šifriranjem od konca do konca, saj je namen slednjega tehnično zagotoviti, da komunikacija ostane zaupna med pošiljateljem in prejemnikom.
99. Čeprav predlog za ponudnike ne določa obveznosti sistematičnega prestrezanja, je tako verjetno, da bi že zgolj možnost izdaje odredbe o zaznavanju močno vplivala na tehnične odločitve ponudnikov, zlasti glede na omejen časovni okvir, ki ga bodo imeli za izpolnitev take odredbe, in visoke kazni, ki bi jim bile naložene, če odredbe ne bi izpolnili.⁷⁸ V praksi bi zaradi tega nekateri ponudniki morda prenehali uporabljati šifriranja od konca do konca.
100. Vpliv poslabšanja šifriranja od konca do konca ali odvrčanja od njegove uporabe, ki je lahko posledica predloga, je treba ustrezno oceniti. Z vsako v spremnem Poročilu o oceni učinka k predlogu predstavljeno tehniko za obidenje ohranjanja zaupnosti, ki je značilnost šifriranja od konca do konca, bi se uvedle vrzeli v varnosti.⁷⁹ Na primer pregledovanje na strani odjemalca⁸⁰ bi verjetno privedlo do precej velikega, neciljno usmerjenega dostopa do nešifriranih vsebin v napravah končnih uporabnikov ter njihove obdelave. Tako znatno poslabšanje zaupnosti bi zlasti prizadelo otroke, saj je verjetneje, da bodo odredbe po zaznavanju usmerjene v storitve, ki jih uporabljajo, zaradi česar bodo izpostavljeni spremljanju ali prisluškovanju. Hkrati je tudi pregledovanje *na strani strežnika* pravzaprav nezdržljivo s paradigmo šifriranja od konca do konca, saj bi bilo treba prekiniti komunikacijski kanal, šifriran vsak z vsakim, kar bi privedlo do množične obdelave osebnih podatkov v strežnikih ponudnikov.
101. Čeprav je v predlagani uredbi navedeno, da „zadevnemu ponudniku prepušča izbiro tehnologij, ki jih uporablja za učinkovito izpolnjevanje odredb o zaznavanju, in se ne bi smela razumeti, kot da spodbuja uporabo katere koli tehnologije ali odvrča od nje,“⁸¹ postane strukturna nezdržljivost nekaterih

⁷⁸ Glej člen 35 predloga.

⁷⁹ Glej oddelek 4.2 v Abelson, Harold, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, John L. Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague in Carmela Troncoso, Bugs in our Pockets: The Risks of Client-Side Scanning (Hrošči v naših žepih: tveganja pri pregledovanju na strani odjemalca), ArXiv, abs/2110.07450 (2021).

⁸⁰ Pregledovanje na strani odjemalca se na splošno nanaša na sisteme, ki pregledujejo vsebine sporočil in iščejo ujemanja z zbirko podatkov o spornih vsebinah, preden je sporočilo poslano predvidenemu prejemniku.

⁸¹ Uvodna izjava 26 predloga.

odredb o zaznavanju s šifriranjem od konca do konca dejansko močna zavora za uporabo šifriranja od konca do konca. Nezmožnost dostopa do storitev in njihove uporabe z uporabo šifriranja od konca do konca (ki je trenutno najodobnejše v smislu tehničnega zagotovila zaupnosti) bi lahko imela zastraševalni učinek na svobodo izražanja in zakonito zasebno uporabo elektronskih komunikacijskih storitev. Škodljivega razmerja med zaznavanjem posnetkov spolne zlorabe otrok in pridobivanja otrok za spolne namene ter šifriranjem od konca do konca se zaveda tudi Komisija, ko v Poročilu o oceni učinka⁸² opozarja, da bi verjetnost, da Facebook leta 2023 začne izvajati šifriranje od konca do konca, pomenila konec Facebookovega prostovoljnega pregledovanja.

102. Da bi se zagotovilo, da predlagana uredba ne bo ogrozila varnosti ali zaupnosti elektronskih komunikacij evropskih državljanov, EOVP in ENVP menita, da bi moralo biti v normativnem delu predloga jasno navedeno, da se ničesar v predlagani uredbi ne bi smelo razlagati tako, da prepoveduje ali slabi šifriranje, v skladu z navedbami v uvodni izjavi 25 začasne uredbe.

4.11 Nadzor, izvrševanje in sodelovanje

4.11.1 Vloga nacionalnih nadzornih organov po Splošni uredbi o varstvu podatkov

103. Predlog določa vzpostavitev mreže nacionalnih usklajevalnih organov, ki so odgovorni za uporabo in izvrševanje predlagane uredbe.⁸³ Čeprav se uvodna izjava 54 predloga glasi: „Pravila iz te uredbe v zvezi z nadzorom in izvrševanjem se ne bi smela razumeti tako, kot da vplivajo na pooblastila in pristojnosti organov za varstvo podatkov iz Uredbe (EU) 2016/679“, EOVP in ENVP menita, da bi bilo treba bolje urediti razmerja med nalogami usklajevalnih organov in organov za varstvo podatkov ter da bi bilo treba organom za varstvo podatkov v predlagani uredbi dati vidnejšo vlogo.
104. Od ponudnikov bi bilo treba zlasti zahtevati, da se pred uporabo katerih koli ukrepov za zaznavanje posnetkov spolne zlorabe otrok ali pridobivanja otrok za spolne namene, ne pa izključno v zvezi z uporabo ukrepov za zaznavanje pridobivanja otrok za spolne namene, kakor je trenutno predvideno s predlogom, posvetujejo z organi za varstvo podatkov v okviru postopka predhodnega posvetovanja iz člena 36 Splošne uredbe za varstvo podatkov.⁸⁴ Za vse ukrepe za zaznavanje bi bilo treba šteti, da sami po sebi povzročajo „veliko tveganje“, zaradi česar bi bilo treba v zvezi z njimi opraviti postopek predhodnega posvetovanja ne glede na to, ali se nanašajo na pridobivanje otrok za spolne namene ali posnetke spolne zlorabe otrok, kakor je že urejeno z začasno uredbo.⁸⁵ Poleg tega bi morali biti pristojni organi za varstvo podatkov, določeni v skladu s Splošno uredbo za varstvo podatkov, vedno, ne pa le v posebnih okoliščinah, pooblaščen za podajanje stališč o predvidenih ukrepih za zaznavanje.⁸⁶
105. Predlagana uredba bi morala vzpostaviti tudi sistem za obravnavo in reševanje nesoglasij med pristojnimi organi in organi za varstvo podatkov glede odredb o zaznavanju. Organi za varstvo podatkov bi zlasti morali imeti pravico izpodbijati odredbo o zaznavanju pred sodišči države članice pristojnega pravosodnega organa ali neodvisnega upravnega organa, ki je izdal odredbo o zaznavanju. Glede tega EOVP in ENVP opozarjata, da po trenutni različici predloga pristojnemu organu pri izdaji odredbe o zaznavanju ni treba upoštevati mnenja pristojnih organov za varstvo podatkov. To bi lahko privedlo do nasprotujočih si odločitev, saj bi organi za varstvo podatkov, kakor je potrjeno s

⁸² Poročilo o oceni učinka, str. 27.

⁸³ Člen 25 predloga.

⁸⁴ Točka (b) druge alineje člena 7(3) predloga.

⁸⁵ Člen 3(1)(c) začasne uredbe.

⁸⁶ Glej točko (c) druge alineje člena 7(3) predloga.

členom 36(2) Splošne uredbe za varstvo podatkov, obdržali celoten sklop popravljalnih pooblastil iz člena 58 Splošne uredbe za varstvo podatkov, vključno s pooblastilom, da odredijo prepoved obdelave.

4.11.2 Vloga EOVP

106. EOVP in ENVP opozarjata, da je v tretjem stavku člena 50(1) predloga določeno, da Center EU pred vključitvijo določene tehnologije na sezname tehnologij, ki bi jih ponudniki storitev gostovanja in ponudniki medosebnih komunikacijskih storitev lahko uporabili za izvrševanje odredb o zaznavanju, „zaprosi za mnenje svoj odbor za tehnologijo in Evropski odbor za varstvo podatkov“. Nadalje je določeno, da EOVP svoje mnenje predloži v osmih tednih, to obdobje pa se lahko glede na kompleksnost vsebine po potrebi podaljša za šest tednov. Nazadnje mora EOVP o vsakem takem podaljšanju obvestiti Center EU v enem mesecu po prejemu zahteve za posvetovanje, skupaj z razlogi za zamudo.
107. Obstoječe naloge EOVP so določene v členu 70 Splošne uredbe za varstvo podatkov in členu 51 Direktive (EU) 2016/680 (v nadaljevanju: direktiva o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj)⁸⁷. V okviru teh nalog je določeno, da na zahtevo Komisije EOVP tej svetuje ter da na njeno zahtevo, na zahtevo nacionalnega nadzornega organa ali svojega predsednika poda mnenja. Čeprav člen 1(3)(d) predloga določa, da ta ne vpliva na pravila, določena v Splošni uredbi za varstvo podatkov ter direktivi o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, dajanje pooblastila Centru EU, da od EOVP zahteva mnenja, presega naloge, dodeljene EOVP po Splošni uredbi za varstvo podatkov ter direktivi o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj. Zato bi bilo treba v predlagani uredbi, vsaj v uvodni izjavi, pojasniti, da predlog širi naloge EOVP. V zvezi s tem EOVP in ENVP cenita pomembno vlogo, ki jo predlog dodeljuje EOVP s tem, ko zahteva njegovo vključitev v praktično izvajanje predlagane uredbe. Sekretariat EOVP ima v praksi bistveno vlogo pri zagotavljanju analitične, upravne in logistične podpore, potrebne za sprejemanje mnenj EOVP. Da bi se poskrbelo, da bodo EOVP in njegovi člani lahko izpolnjevali svoje naloge, je zato bistveno EOVP dodeliti dovolj proračunskih sredstev in osebja. Kljub temu v oceni finančnih posledic predloga žal ni navedeno, da bi bili za izvajanje dodatnih nalog, ki jih predlog dodeljuje EOVP, dani na voljo kakršni koli dodatni viri.⁸⁸
108. Poleg tega EOVP in ENVP opozarjata, da v členu 50 predloga ni navedeno, kako bo Center EU ravnal po prejemu mnenja EOVP.⁸⁹ V uvodni izjavi 27 predloga je zgolj navedeno, da bi Center EU in Evropska komisija morala upoštevati nasvete EOVP. Zato bi bilo treba pojasniti, kakšen bo namen zahtevanega mnenja v postopku, določenem v členu 50, in kako naj Center EU ravna po prejemu mnenja EOVP.
109. EOVP in ENVP tudi menita, da čeprav se bodo z morebitnimi smernicami EOVP ali njegovim morebitnim mnenjem o uporabi tehnologij za zaznavanje ocenila uporaba takih tehnologij na splošni ravni, bo nacionalni nadzorni organ za predhodno posvetovanje v skladu s členom 36 Splošne uredbe za varstvo podatkov moral upoštevati konkretne okoliščine in za vsak primer posebej oceniti

⁸⁷ Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ, ULL 119, 4. 5. 2016, str. 89–131.

⁸⁸ Glej predlog, str. 105 in naslednje.

⁸⁹ Glej nasprotno člen 51(4) direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj.

predvideno obdelavo zadevnega upravljavca. EOVP in ENVP opozarjata, da bodo nadzorni organi pri odločanju, ali je treba podaljšati rok za predložitev njihovih mnenj v odgovor na predhodno posvetovanje, določen v Splošni uredbi za varstvo podatkov, uporabili in da bi morali uporabiti merila iz člena 36 Splošne uredbe za varstvo podatkov ter da ni potrebe po uporabi drugačnih standardov, kadar se predhodno posvetovanje nanaša na uporabo tehnologije za zaznavanje.⁹⁰

110. Nazadnje predlog pri uporabi člena 11 (Smernice v zvezi z obveznostmi zaznavanja) določa, da lahko Komisija izda smernice o uporabi členov 7 do 10 predloga. Člen 11 predloga bi bilo treba spremeniti tako, da se pojasni, da bi se Komisija pred izdajo smernic v zvezi z obveznostmi zaznavanja poleg usklajevalnih organov in Centra EU morala glede osnutka smernic posvetovati z EOVP zunaj predvidenega postopka javnega posvetovanja.
111. Zato ta naloga EOVP ter njegova vloga v pravnem okviru, ki bi jo uvedel predlog, upravičujeta nadaljnjo oceno zakonodajalca.

4.11.3 Vloga Centra EU za boj proti spolni zlorabi otrok

112. V skladu s poglavjem IV predloga bi se kot nova decentralizirana agencija, ki bi omogočila izvajanje predloga, vzpostavil Center EU. Center EU naj bi poleg drugih nalog ponudnikom olajšal dostop do zanesljivih tehnologij za zaznavanje, dal na voljo kazalnike, ustvarjene na podlagi spolne zlorabe otrok na spletu, kot jo preverijo sodišča ali neodvisni upravni organi držav članic, za namen zaznavanja, na zahtevo nudil ustrezno pomoč v zvezi z izvajanjem ocen tveganja in zagotavljal podporo pri komunikaciji z ustreznimi nacionalnimi organi.⁹¹
113. V zvezi s tem EOVP in ENVP pozdravljata člen 77(1) predloga, s katerim je potrjeno, da mora Center EU osebne podatke obdelovati v skladu z uredbo EUDPR, in predpisano, da se po posvetovanju z ENVP določijo ukrepi, na podlagi katerih Center EU uporablja navedeno uredbo, vključno z ukrepi v zvezi z imenovanjem uradne osebe za varstvo podatkov v Centru EU. Kljub temu EOVP in ENVP menita, da je treba več določb tega poglavja podrobneje pregledati.
114. Prvič, EOVP in ENVP opozarjata, da člen 48 predloga predpisuje posredovanje vsake naznanitve, ki „ni očitno neutemeljena“⁹², nacionalnim organom kazenskega pregona ter Agenciji Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (v nadaljevanju: Europol). Ta prag, po katerem Center EU nacionalnim organom kazenskega pregona in Europolu posreduje vsako naznanitev (ki „ni očitno neutemeljena“), se zdi prenizek, zlasti ob upoštevanju, da je namen vzpostavitve Centra EU, kakor je določen v Poročilu Komisije o oceni učinka,⁹³ razbremeniti organe kazenskega pregona in Europol filtriranja vsebin, ki so napačno označene kot posnetki spolne zlorabe otrok. Glede tega ni jasno, zakaj Center EU kot središče strokovnega znanja in izkušenj ne bi mogel opraviti temeljitejše pravne in dejanske ocene, da se zmanjšajo tveganja za prenos podatkov nedolžnih oseb organom kazenskega pregona.
115. Drugič, zdi se, da je določba, ki se nanaša na trajanje hrambe osebnih podatkov pri Centru EU, glede na občutljivost zadevnih podatkov razmeroma odprta. Tudi če ne bi bilo mogoče določiti najdaljšega

⁹⁰ Glej uvodno izjavo 24.

⁹¹ Glej COM(2022) 209 final, str. 7.

⁹² Izraz „očitno neutemeljene“ je v uvodni izjavi 65 predloga opisan kot „pri katerih je takoj, brez kakršne koli vsebinske pravne ali dejanske analize, razvidno, da prijavljene dejavnosti ne pomenijo spolne zlorabe otrok na spletu.“

⁹³ Glej na primer stran 349 Poročila o oceni učinka.

časa hrambe navedenih podatkov, EOVP in ENVP priporočata, da se v predlogu določi vsaj najkrajši rok za pregled potrebnosti nadaljnje hrambe podatkov in za utemeljitev podaljšane hrambe po navedenem obdobju.

116. Poleg tega glede na zelo veliko občutljivost osebnih podatkov, ki jih bo obdeloval Center EU, EOVP in ENVP menita, da bi za obdelavo morali veljati dodatni zaščitni ukrepi, zlasti da se zagotovi učinkovit nadzor. To bi lahko vključevalo obveznost Centra EU, da vodi dnevnik dejanj obdelave v sistemih za avtomatizirano obdelavo, ki se nanašajo na navedene podatke (tj. podobno kot zahteva glede operativnih osebnih podatkov iz poglavja IX uredbe EUDPR), vključno z beleženjem vnosa, spremembe, dostopa, vpogleda, razkritja, kombiniranja in izbrisa osebnih podatkov. Dnevnik vpogleda in razkritja omogočajo, da se take dejavnosti utemeljijo, da se opredeli datum in čas takih dejavnosti ter identificirajo osebe, ki so vpogledale v operativne osebne podatke ali jih razkile, ter da se, kolikor je to mogoče, identificirajo uporabniki. Ti dnevnik bi se uporabljali za preverjanje zakonitosti obdelave, notranje spremljanje ter zagotavljanje celovitosti in varnosti operativnih osebnih podatkov, uradni osebi Centra EU za varstvo podatkov in ENVP pa bi se dostop do njih omogočil na zahtevo.
117. Poleg tega je v predlogu navedena obveznost ponudnikov, da uporabnike obvestijo o zaznavanju posnetkov spolne zlorabe otrok prek odredb o zaznavanju in o pravici do vložitve pritožbe pri usklajevalnem organu.⁹⁴ Kljub temu predlog ne določa postopkov za uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki, tudi ob upoštevanju več lokacij, kamor so osebni podatki lahko preneseni in kjer so lahko shranjeni v skladu s predlogom (Center EU, Europol, nacionalni organi kazenskega pregona). Zahteva glede obveščanja uporabnikov bi morala vključevati obveznost obveščanja posameznikov, da so, kjer je primerno, različni subjekti posredovali njihove podatke in da jih obdelujejo (na primer da so jih posredovali in da jih obdelujejo organi kazenskega pregona in da jih je prejel Europol). Poleg tega bi moral biti vzpostavljen centraliziran postopek za prejemanje in usklajevanje zahtev glede pravice do dostopa, popravka in izbrisa ali namesto tega obveznost, da se subjekt, ki prejme zahtevo posameznika, na katerega se nanašajo osebni podatki, uskladi z drugimi zadevnimi subjekti.
118. EOVP in ENVP opozarjata, da je naloga Centra EU v skladu s členom 50 predloga pripraviti seznam tehnologij, ki se lahko uporabljajo za izvrševanje odredb o zaznavanju. Kljub temu so v skladu s členom 12(1) predloga ponudniki dolžni naznaniti vse informacije, ki kažejo na morebitno spolno zlorabo otrok na spletu v njihovih storitvah, in ne le tistih, ki izhajajo iz izvrševanja odredbe o zaznavanju. Zelo verjetno je, da bi precejšnja količina teh informacij izhajala iz uporabe ponudnikovih ukrepov za zmanjšanje tveganja v skladu s členom 4 predloga. Zato se zdi ključno določiti, kateri bi bili ti ukrepi, kakšna bi bila njihova učinkovitost, stopnja napake pri naznanjanju morebitne spolne zlorabe otrok ter kakšen je njihov vpliv na pravice in svoboščine posameznikov. Kljub dejstvu, da je v členu 4(5) predloga navedeno, da lahko Komisija v sodelovanju z usklajevalnimi organi in Centrom EU ter po izvedbi javnega posvetovanja izda ustrezne smernice, se EOVP in ENVP zdi pomembno, da zakonodajalec v člen 50 vključi nalogo Centra EU, da zagotovi tudi seznam priporočenih ukrepov za zmanjšanje tveganja in ustreznih dobrih praks, ki so zlasti uspešni pri prepoznavanju morebitne spolne zlorabe otrok na spletu. Ker lahko taki ukrepi posežejo v temeljne pravice do varstva podatkov in zasebnosti, je priporočljivo tudi, da Center EU pred izdajo takega seznama zaprosi EOVP za mnenje.

⁹⁴ Glej člen 10(6) in po naznanitvi Centru EU člen 12(2) predloga.

119. Nazadnje bi morale biti varnostne zahteve iz člena 51(4) predloga natančnejše. Glede tega je mogoče navdih najti pri varnostnih zahtevah, določenih v drugih uredbah glede obsežnih sistemov, ki vključujejo visokotvegano obdelavo, kot so Uredba 767/2008⁹⁵ (glej člen 32), Uredba 1987/2006⁹⁶ (glej člen 16), Uredba 2018/1862⁹⁷ (glej člen 16) in Uredba 603/2013⁹⁸ (glej člen 34).

4.11.4 Vloga Europol

120. Predlog določa tesno sodelovanje med Centrom EU in Europolom. V skladu s poglavjem IV predloga Center EU ob prejemu naznanitev ponudnikov o domnevnih posnetkih spolne zlorabe otrok te naznanitve preveri in oceni, katere so uporabne (niso očitno neutemeljene), ter jih posreduje Europolu in nacionalnim organom kazenskega pregona.⁹⁹ Center EU Europolu odobri dostop do svojih podatkovnih zbirk kazalnikov in podatkovnih zbirk naznanitev, da bi Europolu pomagal pri preiskovanju domnevnih kaznivih dejanj spolne zlorabe otrok.¹⁰⁰ Poleg tega bi bil Centru EU odobren „čim bolj popoln“ dostop do Europolovih informacijskih sistemov.¹⁰¹ Agenciji bosta imeli tudi skupne prostore in nekatero (neoperativno) infrastrukturo.¹⁰²
121. EOVP in ENVP opozarjata, da več vidikov v zvezi s sodelovanjem med predlaganim Centrom EU in Europolom vzbuja pomisleke ali potrebuje podrobnejšo opredelitev.

O posredovanju naznanitev Europolu s strani Centra EU (člen 48)

122. Člen 48 predlagane uredbe predpisuje, da Center EU naznanitve, za katere meni, da niso očitno neutemeljene, skupaj z vsemi dodatnimi ustreznimi informacijami posreduje Europolu in pristojnemu organu ali organom kazenskega pregona države članice, ki bi lahko bili pristojni za preiskavo ali pregon morebitne spolne zlorabe otrok. Čeprav ta člen Europolu dodeljuje vlogo določitve ustreznega organa kazenskega pregona, kadar zadevna država članica ni jasna, je z določbo dejansko predpisano, da se

⁹⁵ Uredba (ES) št. 767/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov med državami članicami o vizumih za kratkoročno prebivanje (Uredba VIS), UL L 218, 13. 8. 2008, str. 60–81.

⁹⁶ Uredba (ES) št. 1987/2006 Evropskega Parlamenta in Sveta z dne 20. decembra 2006 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II), UL L 381, 28. 12. 2006, str. 4–23.

⁹⁷ Uredba (EU) 2018/1862 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah, o spremembi in razveljavitvi Sklepa Sveta 2007/533/PNZ ter o razveljavitvi Uredbe (ES) št. 1986/2006 Evropskega parlamenta in Sveta in Sklepa Komisije 2010/261/EU, UL L 312, 7. 12. 2018, str. 56–106.

⁹⁸ Uredba (EU) št. 603/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o vzpostavitvi sistema Eurodac za primerjavo prstnih odtisov zaradi učinkovite uporabe Uredbe (EU) št. 604/2013 o vzpostavitvi meril in mehanizmov za določitev države članice, odgovorne za obravnavanje prošnje za mednarodno zaščito, ki jo v eni od držav članic vložijo državljani tretje države ali oseba brez državljanstva, in o zahtevah za primerjavo s podatki iz sistema Eurodac, ki jih vložijo organi kazenskega pregona držav članic in Europol za namene kazenskega pregona, ter o spremembi Uredbe (EU) št. 1077/2011 o ustanovitvi Evropske agencije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (prenovitev), UL L 180, 29. 6. 2013, str. 1–30.

⁹⁹ Glej člen 48 predloga.

¹⁰⁰ Glej člen 46(4)–(5) predloga.

¹⁰¹ Glej člen 53(2) predloga.

¹⁰² Predvsem tiste zvezi z upravljanjem človeških virov, informacijsko tehnologijo (IT), vključno s kibernetiko varnostjo, stavbo in komunikacijami.

Europolu posredujejo vse naznanitve ne glede na to, ali je Center EU nacionalni organ opredelil in mu naznanitev že posredoval.

123. Kljub temu predlog ne pojasnjuje, kakšna bi bila dodana vrednost Europolove vključenosti ali pričakovane vloge ob prejemu naznanitev, zlasti v primerih, ko je bil nacionalni organ kazenskega pregona opredeljen in hkrati obveščen.¹⁰³
124. EOVP in ENVP opozarjata, da je Europolova pristojnost omejena na podpiranje dejavnosti pristojnih organov držav članic ter njihovo medsebojno sodelovanje pri preprečevanju hudih kaznivih dejanj, ki prizadenejo dve ali več držav članic, in boju proti njim.¹⁰⁴ Člen 19 Uredbe (EU) 2016/794¹⁰⁵, kakor je bil spremenjen z Uredbo (EU) 2022/991¹⁰⁶ (v nadaljevanju: spremenjena uredba o Europolu), predpisuje, da je organ Unije, ki Europolu zagotavlja informacije, dolžan določiti namen oziroma namene, za katere Europol obdeluje te informacije, in pogoje obdelave. Poleg tega je tudi odgovoren za zagotavljanje točnosti prenesenih osebnih podatkov.¹⁰⁷
125. Splošno posredovanje naznanitev Europolu bi bilo tako v nasprotju s spremenjeno uredbo o Europolu in bi prineslo številna tveganja za varstvo podatkov. Podvajanje obdelave osebnih podatkov bi lahko privedlo do več hkrati shranjenih kopij enakih zelo občutljivih osebnih podatkov (na primer pri Centru EU, Europolu, nacionalnem organu kazenskega pregona), kar bi zaradi morebitne izgube sinhroniziranosti podatkovnih zbirk pomenilo tveganja za točnost podatkov, pa tudi za uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki. Poleg tega s predlogom vzpostavljeni nizki prag za izmenjavo naznanitev z organi kazenskega pregona (tistih, ki „niso očitno neutemeljene“) pomeni veliko verjetnost, da bodo v Europolovih informacijskih sistemih za dalj časa shranjeni lažno pozitivni rezultati (tj. vsebine, napačno označene kot spolna zloraba otrok).¹⁰⁸
126. Zato EOVP in ENVP priporočata, da se v predlogu navedejo ter omejijo okoliščine in nameni, na podlagi katerih bi Center EU lahko Europolu posredoval naznanitve v skladu s spremenjeno uredbo o Europolu. Pri tem bi morale biti izrecno izvzete tiste okoliščine, v katerih so naznanitve poslane ustreznemu organu kazenskega pregona države članice in ki ne pomenijo čezmejnih posledic. Poleg tega bi predlog moral vključevati zahtevo, da Center EU Europolu prenese le osebne podatke, ki so ustrezni, relevantni in omejeni na to, kar je nujno potrebno. Določiti je treba tudi konkretne zaščitne ukrepe za zagotavljanje kakovosti in zanesljivosti podatkov.

¹⁰³ V uvodni izjavi 71 predloga se le v splošnem omenjajo Europolove izkušnje z opredelitvijo pristojnih nacionalnih organov v nejasnih primerih ter njegova podatkovna zbirka kriminalističnih obveščevalnih podatkov, ki lahko prispeva k odkrivanju povezav s preiskavami v drugih državah članicah.

¹⁰⁴ Glej člen 3 spremenjene uredbe o Europolu.

¹⁰⁵ Uredba (EU) 2016/794 Evropskega parlamenta in Sveta z dne 11. maja 2016 o Agenciji Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol) ter nadomestitvi in razveljavitvi sklepov Sveta 2009/371/PNZ, 2009/934/PNZ, 2009/935/PNZ, 2009/936/PNZ in 2009/968/PNZ, UL L 135, 24. 5. 2016, str. 53–114.

¹⁰⁶ Uredba (EU) 2022/991 Evropskega parlamenta in Sveta z dne 8. junija 2022 o spremembi Uredbe (EU) 2016/794 v zvezi s sodelovanjem Europol z zasebnimi strankami, obdelavo osebnih podatkov s strani Europol pri podpiranju preiskav kaznivih dejanj in vlogo Europol pri raziskavah in inovacijah, UL L 169, 27. 6. 2022, str. 1–42.

¹⁰⁷ Člen 38(2)(a) spremenjene uredbe o Europolu.

¹⁰⁸ Po navedbah iz Poročila Komisije o oceni učinka je Europol uspel pregledati le 20 odstotkov od 50 milijonov edinstvenih slik in videoposnetkov spolne zlorabe otrok iz svoje podatkovne zbirke, kar kaže na pomanjkanje virov za obravnavo posnetkov spolne zlorabe otrok, ki jih trenutno prejema. Glej Poročilo o oceni učinka, spremni dokument k predlogu uredbe o določitvi pravil za preprečevanje spolne zlorabe otrok in boj proti njej, SWD(2022) 209, str. 47–48.

Člen 53(2) o tesnem sodelovanju med Centrom EU in Europolom

127. Člen 53(2) predloga določa, da Europol in Center EU drug drugemu zagotovita „čim bolj popoln dostop do ustreznih [...] informacijskih sistemov, kadar je to potrebno za opravljanje njunih nalog in v skladu z akti prava Unije, ki urejajo tak dostop.“
128. V členih 46(4) in 46(5) predloga je še navedeno, da ima Europol dostop do podatkovne zbirke kazalnikov in podatkovne zbirke naznanitev Centra EU, v členu 46(6) pa je določen postopek za odobritev tega dostopa: Europol vloži zahtevo, v kateri navede namen in raven dostopa, ki je potrebna za doseg tega namena, Center EU pa zahtevo ustrezno oceni.
129. Merila in zaščitni ukrepi, ki pogojujejo Europolov dostop do podatkov, pridobljenih iz informacijskih sistemov Centra EU, in njihovo nadaljnjo uporabo, niso navedeni. Poleg tega ni pojasnjeno, zakaj je treba Europolu odobriti neposreden dostop do informacijskih sistemov organov, ki niso organi kazenskega pregona, pri čemer ti sistemi vsebujejo zelo občutljive osebne podatke, katerih povezava s kriminalno dejavnostjo in preprečevanjem kriminalitete morda ni ugotovljena. Da se zagotovita visoka stopnja varstva podatkov in skladnost z načelom omejitve namena, EOVP in ENVP priporočata, da prenos podatkov med Centrom EU in Europolom poteka le prek komunikacijskega orodja za varno izmenjavo, kot je omrežje SIENA, za vsak primer posebej in na podlagi ustrezno ocenjene zahteve.¹⁰⁹
130. Dostop Centra EU do Europolovih informacijskih sistemov je omenjen le v členu 53(2) predloga. Zato ni jasno, za katere namene in v skladu s katerimi konkretnimi zaščitnimi ukrepi bi tak dostop potekal.
131. EOVP in ENVP opozarjata, da je Europol organ kazenskega pregona, ki je bil ustanovljen na podlagi Pogodb EU, njegova temeljna pristojnost pa se nanaša na preprečevanje hudih kaznivih dejanj in boj proti njim. Posledično za operativne osebne podatke, ki jih obdeluje Europol, veljajo stroga pravila o obdelavi podatkov in zaščitni ukrepi v zvezi z njo. Predlagani Center EU ni organ kazenskega pregona in v nobenem primeru mu ne bi smel biti odobren neposreden dostop do Europolovih informacijskih sistemov.
132. EOVP in ENVP še opozarjata, da se bo velik delež informacij, ki so v skupnem interesu Centra EU in Europola, nanašal na osebne podatke, ki se nanašajo na žrtve domnevnih kaznivih dejanj, osebne podatke mladoletnikov in osebne podatke, ki se nanašajo na spolno življenje, ti podatki pa po spremenjeni uredbi o Europolu spadajo med posebne vrste osebnih podatkov. Spremenjena uredba o Europolu postavlja stroge pogoje glede dostopa do posebnih vrst osebnih podatkov. Člen 30(3) spremenjene uredbe o Europolu določa, da ima neposreden dostop do takih osebnih podatkov le Europol, natančneje le omejeno število Europolovih uradnikov, ki jim izvršni direktor dovoli tak dostop.¹¹⁰
133. Zato EOVP in ENVP priporočata, da se besedilo člena 53(2) predloga pojasni tako, da pravilno izraža omejitve, vzpostavljene na podlagi spremenjene uredbe o Europolu, in opredeli načine dostopa Centra EU. Zlasti bi moral biti vsak dostop do osebnih podatkov, ki se obdelujejo v Europolovih informacijskih sistemih, kadar se zdi, da je tak dostop nujno potreben za izvajanje nalog Centra EU, odobren le za vsak primer posebej, in sicer na podlagi predložitve izrecne zahteve, v kateri sta navedena konkretni namen in utemeljitev. Europol bi moral skrbno oceniti navedene zahteve in

¹⁰⁹ Mrežna aplikacija za varno izmenjavo informacij (SIENA).

¹¹⁰ V skladu s spremenjeno uredbo o Europolu veljajo za agencije Unije, ustanovljene na podlagi naslova V PDEU, izjeme od te prepovedi. Vendar glede na pravno podlago predloga (člen 114 PDEU, ki se nanaša na usklajevanje notranjega trga) ta izjema ne bi zajela predlaganega Centra EU.

Centru EU prenesti osebne podatke le, kadar je to nujno potrebno in sorazmerno s potrebnim namenom.

Člen 10(6) o Europolovi vlogi pri obveščanju uporabnikov po izvedbi odredbe o zaznavanju

134. EOVP in ENVP pozdravljata zahtevo, kakor je določena v členu 10(6) predloga, da ponudniki obvestijo uporabnike, na katerih osebne podatke se morda nanaša izvršitev odredbe o zaznavanju. Ta obvestitev uporabnikov se opravi šele po pridobitvi potrditve Europolu ali nacionalnega organa kazenskega pregona države članice, ki je v skladu s členom 48 predloga prejel naznanitev, da obvestitev uporabnikov ne bo posegla v dejavnosti preprečevanja, zaznavanja, preiskovanja in pregona kaznivih dejanj spolne zlorabe otrok.
135. Kljub temu so podrobnosti glede praktičnega izvajanja te določbe pomanjkljive. Predlog ne določa, ali je v primerih, ko se naznanitve posredujejo tako Europolu kot tudi organu kazenskega pregona države članice, potrebna potrditev enega ali obeh prejemnikov, poleg tega pa v predlogu niso navedeni postopki oziroma načini za pridobitev te potrditve (na primer ali naj se potrditve usmerjajo prek Centra EU). Ob upoštevanju velike količine posnetkov spolne zlorabe otrok, ki bi jih Europol in nacionalni organi kazenskega pregona morda morali obdelati, ter pomanjkanja točnega roka za potrditev („brez nepotrebnega odlašanja“) EOVP in ENVP priporočata, da se upoštevni postopki pojasnijo, da bi se zagotovilo uresničevanje tega zaščitnega ukrepa v praksi. Poleg tega bi obveznost obvestitve uporabnikov morala vključevati tudi informacije glede prejemnikov zadevnih osebnih podatkov.

O zbiranju podatkov in poročanju o preglednosti (člen 83)

136. Člen 83(3) predloga določa, da Center EU zbira podatke in pripravlja statistiko v zvezi z več svojimi nalogami iz predlagane uredbe. EOVP in ENVP priporočata, da se za namene spremljanja temu seznamu doda statistika o številu naznanitev, posredovanih Europolu v skladu s členom 48, in številu zahtev za dostop, ki jih Europol prejme na podlagi členov 46(4) in 46(5), vključno s številom zahtev, ki jim Center EU ugodí in ki jih zavrne.

5. SKLEPNA UGOTOVITEV

137. Čeprav EOVP in ENVP pozdravljata prizadevanja Komisije, da zagotovi učinkovito ukrepanje zoper spolno zlorabo otrok na spletu, menita, da predlog vzbuja resne pomisleke glede varstva podatkov in zasebnosti. Zato bi EOVP in ENVP pozvala zakonodajalca, naj predlagano uredbo spremenita, zlasti tako, da bi predvidene obveznosti zaznavanja dosegle upoštevne standarde glede potrebnosti in sorazmernosti ter ne bi privedle do oslabitve ali poslabšanja šifriranja na splošni ravni. EOVP in ENVP sta pripravljena ponuditi podporo v okviru zakonodajnega postopka, če se bo zdelo, da je njun prispevek potreben za obravnavo pomislekov, poudarjenih v tem skupnem mnenju.

Za Evropskega nadzornika za varstvo podatkov

Evropski nadzornik za varstvo podatkov

(Wojciech Wiewiorowski)

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)