

PRIPOROČILA

PRIPOROČILO KOMISIJE (EU) 2018/334

z dne 1. marca 2018

o ukrepih za učinkovito preprečevanje nezakonitih spletnih vsebin

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 292 Pogodbe,

ob upoštevanju naslednjega:

- (1) Internet in ponudniki storitev, ki so dejavni na internetu, pomembno prispevajo k inovacijam, gospodarski rasti in ustvarjanju delovnih mest v Uniji. Mnogi od teh ponudnikov storitev imajo odločilno vlogo v digitalnem gospodarstvu, saj povezujejo podjetja in državljane ter omogočajo javne razprave ter razširjanje in sprejemanje informacij o dejstvih, mnenj in idej. Vendar pa njihove storitve v nekaterih primerih zlorabijo tretje osebe za izvajanje nezakonitih dejavnosti na spletu, na primer razširjanje nekaterih informacij v zvezi s terorizmom, spolno zlorabo otrok, nezakonitim sovražnim govorom ali kršitvami zakonodaje o varstvu potrošnikov, ki bi lahko porušile zaupanje njihovih uporabnikov in škodovala njihovim poslovnim modelom. V nekaterih primerih zadevni ponudniki storitev morda celo iztržijo nekaj koristi od te dejavnosti, na primer zaradi razpoložljivosti avtorsko zaščitene vsebin brez dovoljenja imetnikov pravic.
- (2) Prisotnost nezakonitih spletnih vsebin ima resne negativne posledice za uporabnike, za druge prizadete državljane in podjetja ter družbo na splošno. Glede na osrednjo vlogo ponudnikov spletnih storitev ter tehnološka sredstva in zmogljivosti, povezane s storitvami, ki jih zagotavljajo, imajo ponudniki spletnih storitev posebno družbeno odgovornost za boj proti nezakonitim vsebinam, ki se razširjajo z uporabo njihovih storitev.
- (3) Glede na to, da je hitra odstranitev nezakonitih vsebin ali onemogočanje dostopa do njih pogosto bistveno za omejitev nadaljnjega razširjanja in škode, navedena odgovornost med drugim pomeni, da bi morali biti zadevni ponudniki storitev zmožni sprejeti hitro odločitev o morebitnih ukrepih v zvezi z nezakonitimi spletnimi vsebinami. Navedena odgovornost pomeni tudi, da bi morali vzpostaviti učinkovite in ustrezne zaščitne ukrepe, zlasti za zagotovitev, da ravnajo skrbno in sorazmerno ter da se prepreči nenamerna odstranitev vsebin, ki niso nezakonite.
- (4) Številni ponudniki spletnih storitev so priznali to odgovornost in v skladu z njo tudi ukrepajo. Na kolektivni ravni je bil dosežen pomemben napredek s prostovoljnimi dogovori različnih vrst, vključno z internetnim forumom EU o terorističnih spletnih vsebinah, kodeksom ravnanja na področju boja proti nezakonitemu sovražnemu govoru na spletu ter memorandumom o soglasju glede prodaje ponarejenega blaga. Vendar kljub tem zavezam in napredku nezakonite spletne vsebine še vedno ostajajo resen problem v Uniji.
- (5) Zaskrbljen zaradi terorističnih napadov v EU in širjenja spletne teroristične propagande je Evropski svet na zasedanju 22. in 23. junija 2017 izjavil, da „za zadevni sektor pričakuje, da bo [...] razvil novo tehnologijo in orodja za izboljšanje samodejnega odkrivanja in odstranjevanja vsebine, ki ščuva k terorističnim dejanjem. [...]“ Evropski parlament je v svoji resoluciji z dne 15. junija 2017 pozval navedene spletne platforme, „naj okrepijo ukrepe za boj proti nezakonitim in škodljivim spletnim vsebinam“. Ministri držav članic so v okviru internetnega foruma EU ponovno pozvali podjetja, naj sprejmejo bolj proaktiven pristop k zaščiti svojih uporabnikov pred terorističnimi vsebinami. Kar zadeva pravice intelektualne lastnine, je Svet v svojih sklepih z dne 4. decembra 2014 o uveljavljanju teh pravic pozval Komisijo, naj preuči uporabo orodij, ki so na voljo za identifikacijo kršiteljev pravic intelektualne lastnine, in vlogo posrednikov pri boju proti kršitvam pravic intelektualne lastnine.

- (6) Komisija je 28. septembra 2017 sprejela sporočilo s smernicami o odgovornosti ponudnikov spletnih storitev v zvezi z nezakonitimi spletnimi vsebinami ⁽¹⁾. V tem sporočilu je Komisija pojasnila, da bo ocenila, ali so potrebni dodatni ukrepi, med drugim s spremljanjem napredka na podlagi prostovoljnih dogovorov. To priporočilo je nadgradnja navedenega sporočila ter odraža raven ambicij, začrtanih v sporočilu, in jih uveljavlja, pri čemer v celoti upošteva pomemben napredek, ki je bil dosežen na podlagi navedenih prostovoljnih dogovorov, in na njem gradi.
- (7) To priporočilo potrjuje, da bi bilo treba ustrezno upoštevati posebnosti boja proti različnim vrstam nezakonitih spletnih vsebin in specifičen odziv, ki bi bil potreben, vključno z namenskimi zakonodajnimi ukrepi. Komisija priznava potrebo po takšnih posebnih zakonodajnih ukrepih, zato je, glede na spreminjajoče se tržne razmere, na primer 25. maja 2016 sprejela predlog za spremembo Direktive 2010/13/EU Evropskega parlamenta in Sveta ⁽²⁾. Poleg tega je 14. septembra 2016 sprejela predlog direktive o avtorskih pravicah na enotnem digitalnem trgu ⁽³⁾, ki vključuje obveznost, da določeni ponudniki storitev v sodelovanju z imetniki pravic sprejmejo ukrepe za zagotovitev izvajanja sporazumov za uporabo njihovih del ali drugih predmetov urejanja ali za preprečitev razpoložljivosti del ali drugih predmetov urejanja v okviru njihovih storitev, ki so jih imetniki pravic ugotovili v sodelovanju s ponudniki storitev. To priporočilo ne vpliva na tovrstne zakonodajne ukrepe in predloge.
- (8) Direktiva 2000/31/ES Evropskega parlamenta in Sveta ⁽⁴⁾ vsebuje izjeme glede odgovornosti, ki so pod določenimi pogoji na voljo za nekatere ponudnike spletnih storitev, ki vključujejo ponudnike storitev gostovanja v smislu člena 14 Direktive. Da bi lahko izkoristili navedeno izjemo glede odgovornosti, morajo ponudniki storitev gostovanja hitro ukrepati in odstraniti nezakonito informacijo, ki jo hranijo, ali onemogočiti dostop do nje, in sicer takoj ko so zanje izvedeli, kar zadeva odškodninske zahtevke pa, odkar so jim znana dejstva ali okoliščine, iz katerih je očitno, da gre za nezakonito dejavnost ali informacijo. Takšno znanje in zavedanje lahko med drugim pridobijo prek prijav, ki so jim bile predložene. Direktiva 2000/31/ES je podlaga za oblikovanje postopkov za odstranitev nezakonitih informacij in onemogočanje dostopa do njih. Navedena direktiva dopušča tudi možnost za države članice, da od zadevnih ponudnikov storitev zahtevajo, da postopajo s skrbnostjo v zvezi z nezakonitimi vsebinami, ki bi jih morda hranili.
- (9) Pri sprejemanju ukrepov v zvezi z nezakonitimi spletnimi vsebinami države članice spoštujejo načelo države izvora iz Direktive 2000/31/ES. V skladu s tem načelom države članice ne smejo iz razlogov, ki spadajo v koordinirano področje, kot je določeno v navedeni direktivi, omejevati svobode zagotavljanja storitev informacijske družbe, ki jih ponujajo ponudniki s sedežem v drugi državi članici, pri čemer so možna odstopanja pod pogoji, določenimi v navedeni direktivi.
- (10) Poleg tega več drugih zakonodajnih aktov Unije zagotavlja pravni okvir v zvezi z nekaterimi vrstami nezakonitih vsebin, ki so na voljo na spletu in se prek njega razširjajo. Zlasti Direktiva 2011/93/EU Evropskega parlamenta in Sveta ⁽⁵⁾ zahteva, da države članice sprejmejo ukrepe za odstranitev spletnih strani, ki vsebujejo ali širijo otroško pornografijo, in dopušča preprečitev dostopa do takšnih spletnih strani, ob upoštevanju nekaterih zaščitnih ukrepov. Direktiva (EU) 2017/541 Evropskega parlamenta in Sveta ⁽⁶⁾, ki jo je treba prenesti v nacionalno zakonodajo do 8. septembra 2018, vsebuje podobne določbe glede spletnih vsebin, ki pomenijo javno ščuvanje k storitvi terorističnega kaznivega dejanja. Direktiva (EU) 2017/541 prav tako določa minimalna pravila glede opredelitve kaznivih dejanj na področju terorističnih kaznivih dejanj, kaznivih dejanj v povezavi s teroristično

⁽¹⁾ COM(2017) 555 final z dne 28. septembra 2017.

⁽²⁾ Direktiva 2010/13/EU Evropskega parlamenta in Sveta z dne 10. marca 2010 o usklajevanju nekaterih zakonov in drugih predpisov držav članic o opravljanju avdiovizualnih medijskih storitev (Direktiva o avdiovizualnih medijskih storitvah) (UL L 95, 15.4.2010, str. 1). COM(2016) 287 final.

⁽³⁾ COM(2016) 593 final z dne 14. septembra 2016.

⁽⁴⁾ Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju) (UL L 178, 17.7.2000, str. 1).

⁽⁵⁾ Direktiva 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ (UL L 335, 17.12.2011, str. 1).

⁽⁶⁾ Direktiva (EU) 2017/541 Evropskega parlamenta in Sveta z dne 15. marca 2017 o boju proti terorizmu in nadomestitvi Okvirnega sklepa Sveta 2002/475/PNZ ter o spremembi Sklepa Sveta 2005/671/PNZ (UL L 88, 31.3.2017, str. 6).

skupino in kaznivih dejanj v povezavi s terorističnimi dejavnostmi. V skladu z Direktivo 2004/48/ES Evropskega parlamenta in Sveta ⁽¹⁾ lahko pristojni sodni organi izdajo sodno odredbo zoper posrednike, katerih storitve tretja oseba uporablja za kršenje pravice intelektualne lastnine.

- (11) Poleg prostovoljnih ukrepov, ki so jih sprejeli nekateri ponudniki spletnih storitev, so zlasti glede na navedeno nekatere države članice od sprejetja Direktive 2000/31/ES sprejele pravila o mehanizmi prijave in ukrepanja. Druge države članice razmišljajo o sprejetju takšnih pravil. Ti mehanizmi na splošno omogočajo lažjo prijavo vsebin, za katere prijavitelj meni, da so nezakonite, zadevnemu ponudniku storitev gostovanja („prijava“), na podlagi katere se navedeni ponudnik lahko odloči, ali se s to oceno strinja in ali želi te vsebine odstraniti oziroma onemogočiti dostop do njih („ukrepanje“). Razlike med takšnimi nacionalnimi predpisi se vedno bolj povečujejo. Posledično za zadevne ponudnike storitev lahko veljajo številne pravne zahteve, ki se razlikujejo glede na njihovo vsebino in področje uporabe.
- (12) V interesu notranjega trga in učinkovitosti boja proti nezakonitim spletnim vsebinam ter za ohranitev uravnoteženega pristopa, ki ga želi zagotoviti Direktiva 2000/31/ES, je treba določiti nekatera glavna načela, ki bi morala biti vodilo za dejavnosti držav članic in zadevnih ponudnikov storitev v zvezi s tem.
- (13) Ta načela bi bilo treba določiti in uporabljati ob popolnem spoštovanju temeljnih pravic, ki jih varuje pravni red Unije, in zlasti pravic iz Listine Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: Listina). Nezakonite spletne vsebine bi bilo treba obravnavati z ustreznimi in strogimi zaščitnimi ukrepi, da bi zagotovili zaščito različnih ogroženih temeljnih pravic vseh zadevnih strani. Te pravice glede na konkretni primer lahko vključujejo svobodo izražanja, vključno s svobodo do prejemanja in sporočanja informacij, pravico do spoštovanja zasebnega življenja in do varstva osebnih podatkov ter pravico do učinkovitega sodnega varstva uporabnikov zadevnih storitev. Vključujejo lahko tudi svobodo gospodarske pobude ponudnikov storitev gostovanja, vključno s svobodnim sklepanjem pogodb, ter tudi pravice otrok, pravico do varstva lastnine, vključno z intelektualno lastnino, pravico do človeškega dostojanstva in nediskriminacije nekaterih drugih prizadetih strani. Odločitve, ki jih sprejmejo ponudniki storitev gostovanja, da odstranijo vsebino, ki jo hranijo, ali onemogočijo dostop do nje, bi morale še zlasti ustrezno upoštevati temeljne pravice in legitimne interese uporabnikov ter osrednjo vlogo, ki jo imajo ti ponudniki pri omogočanju javne razprave ter razširjanju in prejemanju dejstev, mnenj ter idej v skladu z zakonom.
- (14) V skladu s horizontalnim pristopom, na katerem temelji izjema glede odgovornosti iz člena 14 Direktive 2000/31/ES, bi se moralo to priporočilo uporabljati za vse vrste vsebin, ki niso v skladu s pravom Unije ali zakonodajo držav članic, ne glede na natančen predmet urejanja ali naravo navedene zakonodaje. Dovolj je, da se upošteva zakonodaja držav članic, ki jih zagotavljanje storitev zadeva, predvsem tistih držav članic, na katerih ozemlju ima ponudnik storitev sedež oziroma na katerem se zagotavljajo storitve. Poleg tega bi bilo treba pri uveljavljanju tega priporočila ustrezno upoštevati resnost nezakonitih vsebin in kakršno koli morebitno škodo, ki jo lahko te vsebine povzročijo in ki je lahko tesno povezana s hitrostjo sprejetja ukrepov, ter kaj je mogoče razumno pričakovati od ponudnikov storitev gostovanja glede na stanje razvoja in možno uporabo tehnologije, če je to primerno. Ustrezno bi bilo treba upoštevati tudi relevantne razlike, ki lahko obstajajo med različnimi vrstami nezakonitih vsebin ter med ukrepi, ki jih je treba sprejeti za njihovo odpravo.
- (15) Ponudniki storitev gostovanja imajo zlasti pomembno vlogo v boju proti nezakonitim spletnim vsebinam, saj na zahtevo svojih uporabnikov hranijo informacije, ki jim jih ti zagotovijo, in drugim uporabnikom omogočajo dostop do njih, pogosto v velikem obsegu. To priporočilo se zato nanaša predvsem na dejavnosti in odgovornosti navedenih ponudnikov. Vendar, kadar je to primerno, se priporočila lahko smiselno uporabljajo tudi v zvezi z drugimi prizadetimi ponudniki spletnih storitev. Glede na to, da je namen tega priporočila, da se obravnavajo tveganja, povezana z nezakonitimi spletnimi vsebinami, ki vplivajo na potrošnike v Uniji, se priporočilo nanaša na dejavnosti vseh ponudnikov storitev gostovanja, ne glede na to, ali imajo sedež v Uniji ali v tretji državi, če je njihova dejavnost usmerjena na potrošnike, ki prebivajo v Uniji.
- (16) Mehanizmi za predložitev prijav ponudnikom storitev gostovanja glede vsebine, ki se šteje za nezakonito, so pomembno sredstvo za boj proti nezakonitim spletnim vsebinam. Takšni mehanizmi bi morali vsem

⁽¹⁾ Direktiva 2004/48/ES Evropskega parlamenta in Sveta z dne 29. aprila 2004 o uveljavljanju pravic intelektualne lastnine (UL L 157, 30.4.2004, str. 45).

posameznikom in subjektom, ki želijo podati prijavo, to omogočati. Zato bi morali biti navedeni mehanizmi vsem uporabnikom lahko dostopni in enostavni za uporabo. Vendar pa bi morali ponudniki storitev gostovanja ohraniti prožnost, na primer v zvezi z obliko poročanja ali tehnologijo, ki se uporabi, da bi se omogočile učinkovite rešitve in da bi se izognili nesorazmernim obremenitvam navedenih ponudnikov.

- (17) V skladu s sodno prakso Sodišča v zvezi s členom 14 Direktive 2000/31/ES bi morale biti prijave dovolj natančne in ustrezno utemeljene, da bi se ponudniku storitev gostovanja, ki te prijave prejmejo, omogočilo sprejeti informirano in premišljeno odločitev glede nadaljnjih ukrepov na podlagi prijave. Zato bi bilo treba v največji možni meri zagotoviti, da so ti standardi doseženi. Ne glede na to, ali prijava vodi do vedenja ali zavedanja v smislu člena 14 navedene direktive, jo je treba obravnavati v luči posebnosti posameznega primera, pri čemer je treba upoštevati, da se takšno vedenje ali zavedanje lahko pridobi tudi na druge načine in ne samo prek prijav.
- (18) Da bi ponudnik storitev gostovanja lahko sprejel informirano in premišljeno odločitev o nadaljnjih ukrepih na podlagi prejete prijave, običajno ne potrebuje kontaktnih podatkov prijavitelja. Če bi bila navedba kontaktnih podatkov obvezen predpogoj za prijavo, bi to pomenilo oviro za podajanje prijav. Vendar pa je vključitev kontaktnih podatkov potrebna, da lahko ponudnik storitev gostovanja zagotovi povratne informacije. Zato bi za prijavitelja morala biti vključitev kontaktnih podatkov možna, vendar ne obvezna.
- (19) Da bi se povečala preglednost in pravilnost mehanizmov prijave in ukrepanja in bi se po potrebi omogočila odprava zadevnih vsebin, bi morali ponudniki storitev gostovanja, če imajo kontaktne podatke o prijaviteljih in/ali ponudnikih vsebin, pravočasno in ustrezno obvestiti navedene osebe o ukrepih, sprejetih v okviru teh mehanizmov, zlasti kar zadeva njihove odločitve o zahtevani odstranitvi zadevnih vsebin ali onemogočenju dostopa do njih. Podatki, ki jih je treba zagotoviti, bi morali biti sorazmerni, in sicer bi morali ustrezati navedbam zadevnih oseb iz njihove prijave ali odgovora na prijavo, pri čemer bi bilo treba omogočiti primerne in raznolike rešitve in ne pretirano obremenjevati ponudnikov.
- (20) Da bi zagotovili preglednost in pravičnost ter da se prepreči nenamerna odstranitev zakonitih vsebin, bi morali biti ponudniki vsebin načeloma obveščeni o odločitvi, da se odstranijo vsebine, ki se hranijo na njihovo zahtevo, ali onemogoči dostop do njih, in imeti možnost izpodbijanja odločitve z odgovorom na prijavo, katerega namen je, kjer je to primerno, razveljavitev odločitve, ne glede na to, ali je bila ta odločitev sprejeta na podlagi prijave ali obvestila ali na podlagi proaktivnih ukrepov ponudnika storitev gostovanja.
- (21) Vendar glede na naravo zadevne vsebine, namen takega postopka z odgovorom na prijavo in dodatno breme, ki ga pomeni za ponudnike storitev gostovanja, ni razloga za priporočilo, da naj bi zagotovili informacije o takšni odločitvi in možnosti izpodbijanja odločitve, če je očitno, da so zadevne vsebine nezakonite in se nanašajo na huda kazniva dejanja, ki ogrožajo življenje ali varnost ljudi, kot so kazniva dejanja, določena v Direktivi (EU) 2017/541 in Direktivi 2011/93/EU. Poleg tega bi v nekaterih primerih razlogi javnega reda in javne varnosti ter zlasti razlogi, povezani s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj, lahko upravičili, da se navedene informacije ne zagotovijo neposredno zadevnemu ponudniku vsebin. Zato ponudniki storitev gostovanja teh ne bi smeli zagotoviti, če je pristojni organ v ta namen vložil zahtevo, ki temelji na razlogih javnega reda in javne varnosti, in sicer vse dokler trajajo navedeni razlogi. Če to povzroči omejitve pravice do obveščeniosti v zvezi z obdelavo osebnih podatkov, bi bilo treba upoštevati ustrezne pogoje iz Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta ⁽¹⁾.
- (22) Mehanizmi prijave in ukrepanja ne bi smeli na noben način vplivati na pravico udeleženih strani, da začnejo sodni postopek v skladu z veljavno zakonodajo, in sicer glede vsebin, ki štejejo za nezakonite, ali kakršnih koli ukrepov, ki jih ponudniki storitev gostovanja sprejmejo v zvezi s tem. Mehanizmi za alternativno reševanje sporov, ki nastanejo v zvezi s tem, so lahko pomembno dopolnilo sodnemu postopku, zlasti kadar omogočajo učinkovito, dostopno in hitro reševanje takih sporov. Alternativno reševanje sporov bi bilo zato treba spodbujati, pod pogojem, da zadevni mehanizmi izpolnjujejo določene standarde, zlasti kar zadeva postopkovno pravičnost, da dostop strank do sodišča ostane neokrnjen in da se preprečijo zlorabe.

⁽¹⁾ 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) (UL L 119, 4.5.2016, str. 1).

- (23) Da bi lahko bolje ocenili učinkovitost mehanizmov prijave in ukrepanja ter drugih dejavnosti ponudnikov storitev gostovanja v zvezi z vsebinami, ki štejejo za nezakonite, in da bi zagotovili odgovornost, bi bilo treba zagotoviti preglednost v odnosu do širše javnosti. Ponudniki storitev gostovanja bi zato morali redno objavljati poročila o navedenih mehanizmih in drugih dejavnosti, ki bi morala biti dovolj popolna in natančna, da omogočajo ustrezen vpogled. Prav tako bi morali predhodno zagotoviti jasnost v svojih pogojih izvajanja storitev in v svojih politikah glede odstranitve kakršnih koli vsebin, ki jih hranijo, vključno z nezakonitimi vsebinami, ali glede onemogočanja dostopa do njih.
- (24) Poleg mehanizmov prijave in ukrepanja so lahko sorazmerni in posebni proaktivni ukrepi, ki jih prostovoljno sprejmejo ponudniki storitev gostovanja, vključno z uporabo avtomatiziranih sredstev v nekaterih primerih, tudi pomemben element v boju proti nezakonitim spletnim vsebinam, brez poseganja v člen 15(1) Direktive 2000/31/ES. V zvezi s takšnimi proaktivnimi ukrepi bi bilo treba upoštevati položaj ponudnikov storitev gostovanja, ki imajo zaradi svoje velikosti ali obsega delovanja omejene vire in strokovno znanje, in potrebo po učinkovitih in ustreznih zaščitnih ukrepih, ki spremljajo take ukrepe.
- (25) Še zlasti je lahko sprejetje takšnih proaktivnih ukrepov primerno, če je nezakonitost vsebin že bila ugotovljena, ali kadar je vrsta vsebin takšna, da njihova umeščenost v kontekst ni bistvena. To je lahko odvisno tudi od narave, obsega in cilja predvidenih ukrepov, vrste zadevnih vsebin, od tega, ali so vsebine prijavili organi pregona ali Europol, in od tega, ali so v zvezi z vsebinami že bili sprejeti ukrepi, ker so vsebine štejele za nezakonite. Ponudniki storitev gostovanja bi morali zlasti v zvezi s posnetki spolnih zlorab otrok sprejeti proaktivne ukrepe za odkrivanje in preprečevanje razširjanja takšnih posnetkov, v skladu z zavezami, ki so jih sprejeli v okviru svetovnega zavezništva proti spolni zlorabi otrok na internetu.
- (26) V zvezi s tem je Komisija v svojem sporočilu z dne 28. septembra 2017 o boju proti nezakonitim spletnim vsebinam določila svoje stališče, da takšni prostovoljni proaktivni ukrepi zadevnega ponudnika storitev gostovanja ne vodijo samodejno do izgube možnosti uporabe izjeme glede odgovornosti iz člena 14 Direktive 2000/31/ES.
- (27) Bistveno je, da za vse ukrepe za boj proti nezakonitim spletnim vsebinam veljajo učinkoviti in ustrezni zaščitni ukrepi, katerih cilj je zagotoviti, da ponudniki storitev gostovanja ravnajo skrbno in sorazmerno pri določanju in izvrševanju svojih politik v zvezi z vsebinami, ki jih hranijo, vključno z nezakonitimi vsebinami, s čimer se zlasti zagotovi, da lahko uporabniki svobodno prejemajo in sporočajo informacije na spletu v skladu s pravom, ki se uporablja. Poleg zaščitnih ukrepov, ki so določeni s pravom, ki se uporablja, na primer v zvezi z varstvom osebnih podatkov, bi bilo treba zagotoviti posebne zaščitne ukrepe, zlasti v obliki človeškega nadzora in preverjanja, ki bi se po potrebi uporabili v zvezi z avtomatiziranimi sredstvi, da bi se preprečila vsaka nenamerna ali napačna odločitev.
- (28) Zagotoviti bi bilo treba neovirano, učinkovito in ustrezno sodelovanje med pristojnimi organi in ponudniki storitev gostovanja pri boju proti nezakonitim spletnim vsebinam. Takšno sodelovanje bi lahko bilo po potrebi deležno pomoči Europol, na primer pri boju proti terorizmu ter spolni zlorabi in spolnemu izkoriščanju otrok, otroški pornografiji in novačenju otrok. Da bi olajšali takšno sodelovanje, bi morali države članice in ponudniki storitev gostovanja imenovati kontaktne točke in treba bi bilo vzpostaviti postopke za obdelavo prijav, ki jih predložijo navedeni organi, in sicer prednostno in s primerno stopnjo zaupanja glede njihove pravilnosti, upoštevajoč posebno strokovno znanje in pristojnosti navedenih organov. Da bi učinkovito obravnavali nekatera posebno huda kazniva dejanja, kot so kazniva dejanja, določena v Direktivi (EU) 2017/541 in Direktivi 2011/93/EU, za katera bi lahko ponudniki storitev gostovanja izvedeli pri opravljanju svoje dejavnosti, bi bilo treba države članice spodbujati k uporabi možnosti iz člena 15(2) Direktive 2000/31/ES, naj zakonsko določijo obveznost poročanja v skladu s pravom, ki se uporablja, zlasti Uredbo (EU) 2016/679.
- (29) Poleg pristojnih organov imajo nekateri posamezniki ali subjekti, vključno z nevladnimi organizacijami in sindikati, lahko tudi posebno strokovno znanje in željo po prostovoljnem prevzemu nekaterih obveznosti v zvezi z bojem proti nezakonitim spletnim vsebinam. Glede na njihovo dodano vrednost in včasih veliko število prijav, bi bilo treba spodbujati sodelovanje med takšnimi zaupanja vrednimi prijavitelji in ponudniki storitev gostovanja, zlasti s prednostno obravnavo prijav, ki jih predložijo, in s primerno stopnjo zaupanja glede njihove pravilnosti.

Vendar pa bi glede na njihov posebni status takšno sodelovanje moralo biti odprto le za posameznike in subjekte, ki spoštujejo vrednote, na katerih temelji Unija, kot so določene v členu 2 Pogodbe o Evropski uniji, in ki izpolnjujejo posamezne ustrezne pogoje, ki bi morali biti tudi jasni, objektivni in javno dostopni.

- (30) Boj proti nezakonitim spletnim vsebinam zahteva celosten pristop, saj takšne vsebine pogosto zlahka prehajajo od enega ponudnika storitev gostovanja k drugemu in pogosto izkoriščajo najšibkejši člen v verigi. Sodelovanje, ki obsega zlasti prostovoljno izmenjavo izkušenj, tehnoloških rešitev in dobrih praks, je zato bistvenega pomena. Takšno sodelovanje je še posebej pomembno za ponudnike storitev gostovanja, ki imajo zaradi svoje velikosti ali obsega delovanja omejene vire in strokovno znanje.
- (31) Terorizem vključuje nezakonito in neselektivno uporabo nasilja in ustrahovanja državljanov. Teroristi so pri razširjanju teroristične propagande vedno bolj odvisni od spleta in pogosto uporabljajo izpopolnjene metode za hitro in široko razširjanje. Čeprav je bil dosežen napredek, zlasti v okviru internetnega foruma EU, še vedno obstaja nujna potreba po zagotovitvi hitrejšega in učinkovitejšega odziva na teroristične spletne vsebine, in sicer poleg potrebe po sodelovanju ponudnikov storitev gostovanja v okviru internetnega foruma EU, da bi v celoti izpolnjevali svoje zaveze glede učinkovitega in celovitega poročanja.
- (32) Ob upoštevanju posebnosti, povezanih z bojem proti terorističnim spletnim vsebinam, bi morala biti priporočila v zvezi z bojem proti nezakonitim vsebinam na splošno dopolnjena z nekaterimi priporočili, ki so še posebej povezana z bojem proti terorističnim spletnim vsebinam, ki bi temeljila na prizadevanjih v okviru internetnega foruma EU in jih krepila.
- (33) Glede na posebej resno tveganje, povezano s terorističnimi vsebinami, in osrednjo vlogo ponudnikov storitev gostovanja pri razširjanju takšnih vsebin, bi morali ponudniki storitev gostovanja sprejeti vse primerne ukrepe, s katerimi ne bi dovoljevali terorističnih vsebin in, če je mogoče, preprečevali njihovo gostovanje, ob upoštevanju svojih zmožnosti za določitev in izvrševanje pogojev izvajanja svojih storitev ter potrebe po učinkovitih in ustreznih zaščitnih ukrepih, in sicer brez poseganja v člen 14 Direktive 2000/31/ES.
- (34) Ti ukrepi bi morali obsegati zlasti sodelovanje s pristojnimi organi in Europolom v zvezi z obvestili, ki so posebna sredstva za obveščanje ponudnikov storitev gostovanja, prilagojena posebnostim boja proti terorističnim vsebinam. Pristojni organi in Europol bi morali pri predložitvi obvestil imeti možnost, da zahtevajo odstranitev vsebin, za katere menijo, da so teroristične, ali onemogočenje dostopa do njih, bodisi s sklicevanjem na ustrezno pravo, ki se uporablja, ali na pogoje izvajanja storitev zadevnega ponudnika storitev gostovanja. Ti mehanizmi obvestil bi morali obstajati poleg mehanizmov za predložitev prijav, vključno s strani zaupanja vrednih prijaviteljev, ki se tudi lahko uporabijo za obveščanje o vsebinah, ki štejejo za teroristične.
- (35) Glede na to, da so teroristične vsebine običajno najbolj škodljive v prvi uri po objavi na spletu in glede na posebno strokovno znanje in odgovornosti pristojnih organov in Eurola, bi bilo treba kot splošno pravilo obvestila oceniti in, kadar je to primerno, se nanje odzvati v eni uri.
- (36) Navedeni ukrepi za boj proti terorističnim vsebinam bi morali obsegati sorazmerne in posebne proaktivne ukrepe, vključno z uporabo avtomatiziranih sredstev, za odkrivanje, prepoznavanje in hitro odstranitev terorističnih vsebin ali za onemogočenje dostopa do njih ter za zagotovitev, da se teroristične vsebine ne pojavijo ponovno, in sicer brez poseganja v člen 15(1) Direktive 2000/31/ES. V zvezi s tem bi bilo treba upoštevati potrebo po ustreznih in učinkovitih zaščitnih ukrepih, ki spremljajo takšne ukrepe, zlasti tistih, ki so priporočeni v poglavju II tega priporočila.
- (37) Sodelovanje med samimi ponudniki storitev gostovanja ter med njimi in pristojnimi organi je izjemno pomembno pri prizadevanjih za odpravo terorističnih spletnih vsebin. Tehnološka orodja, ki omogočajo samodejno zaznavanje vsebin, kot so podatkovna zbirka ključnikov, še zlasti lahko prispevajo k doseganju cilja preprečevanja širjenja terorističnih vsebin po različnih storitvah gostovanja. Takšno sodelovanje ter razvoj, delovanje in izmenjavo takšnih tehnoloških orodij bi bilo treba spodbujati ter po potrebi izkoristiti strokovno znanje Eurola. Ta skupna prizadevanja so še posebej pomembna pri omogočanju, da se lahko ponudniki storitev gostovanja, ki imajo zaradi svoje velikosti ali obsega delovanja omejena sredstva in strokovno znanje, takoj učinkovito odzovejo na obvestilo in sprejmejo proaktivne ukrepe, kot je bilo priporočeno.

- (38) Navedenim skupnim prizadevanjem bi se morale pridružiti čim več zadevnih ponudnikov storitev gostovanja, vsi sodelujoči ponudniki storitev gostovanja pa bi morali prispevati k optimalni in čim večji uporabi navedenih orodij. Spodbujati bi bilo treba tudi sklenitev delovne ureditve med vsemi zadevnimi stranmi, po potrebi vključno z Europolom, saj takšna ureditev lahko pripomore k zagotavljanju doslednega in učinkovitega pristopa ter omogoča izmenjavo ustreznih izkušenj in strokovnega znanja.
- (39) Da se zagotovi spoštovanje temeljne pravice do varstva posameznikov v zvezi z obdelavo osebnih podatkov, kot tudi prost pretok osebnih podatkov, bi morala biti obdelava osebnih podatkov v okviru vseh ukrepov, sprejetih za uveljavitev tega priporočila, popolnoma v skladu s predpisi o varstvu podatkov, zlasti z Uredbo (EU) 2016/679 in Direktivo (EU) 2016/680 Evropskega parlamenta in Sveta ⁽¹⁾, spremljati pa bi jo morali pristojni nadzorni organi.
- (40) To priporočilo spoštuje temeljne pravice in upošteva načela, priznana zlasti v Listini. Še posebej si to priporočilo prizadeva zagotoviti polno spoštovanje členov 1, 7, 8, 10, 11, 16, 17, 21, 24 in 47 Listine.
- (41) Komisija namerava pozorno spremljati vse ukrepe, sprejete kot odziv na to priporočilo. Države članice in ponudniki storitev gostovanja bi zato morali Komisiji na njeno zahtevo predložiti vse ustrezne informacije, za katere je mogoče razumno pričakovati, da jih bodo ponudniki storitev gostovanja predložili, da bi omogočili takšno spremljanje. Na osnovi tako pridobljenih informacij in vseh ostalih razpoložljivih informacij, vključno s poročanjem na podlagi različnih prostovoljnih dogovorov, bo Komisija ocenila učinke tega priporočila ter ugotovila, ali so potrebni dodatni ukrepi, vključno s predlogi za zavezujoče pravne akte Unije. Glede na posebnosti in nujnost boja proti terorističnim spletnim vsebinam, bi morala biti navedena spremljanje in ocenjevanje izvedena na podlagi podrobnih informacij in precej hitro – v treh mesecih od datuma objave tega priporočila –, medtem ko je za druge nezakonite vsebine treba to izvesti v šestih mesecih po objavi –

SPREJELA NASLEDNJE PRIPOROČILO:

POGLAVJE I

Namen in terminologija

1. Države članice in ponudniki storitev gostovanja se v zvezi z vsebinami, ki jih zagotavljajo ponudniki vsebin in ki jih hranijo na njihovo zahtevo, spodbujajo, naj sprejmejo učinkovite, ustrezne in sorazmerne ukrepe za boj proti nezakonitim spletnim vsebinam, v skladu z načeli, določenimi v tem priporočilu, in v popolni skladnosti z Listino EU o temeljnih pravicah, zlasti s pravico do svobodnega izražanja in obveščanja, ter drugimi veljavnimi določbami prava Unije, zlasti v zvezi z varstvom osebnih podatkov, konkurenco in elektronskim poslovanjem.
2. To priporočilo temelji na napredku, doseženem v okviru prostovoljnih dogovorov med ponudniki storitev gostovanja in drugimi prizadetimi ponudniki storitev v zvezi z različnimi vrstami nezakonitih vsebin, in ga krepi. Na področju terorizma to priporočilo temelji na napredku, doseženem v okviru internetnega foruma EU, in ga krepi.
3. To priporočilo ne posega v pravice in obveznosti držav članic, da sprejmejo ukrepe v zvezi z nezakonitimi spletnimi vsebinami v skladu s pravom Unije, vključno z možnostjo, da sodišča ali upravni organi države članice v skladu s svojimi pravnimi sistemi od ponudnikov storitev gostovanja zahtevajo, da odstranijo nezakonite vsebine ali onemogočijo dostop do njih. To priporočilo tudi ne posega v položaj ponudnikov storitev gostovanja v skladu z Direktivo 2000/31/ES in njihovo možnost, da določijo in izvršujejo pogoje izvajanja svojih storitev v skladu s pravom Unije in zakonodajo držav članic.

⁽¹⁾ 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 (UL L 119, 4.5.2016, str. 89).

4. V tem priporočilu so uporabljeni naslednji izrazi:
- (a) „ponudnik storitev gostovanja“ pomeni ponudnika storitev informacijske družbe, ki zajemajo shranjevanje informacij, ki jih zagotovi prejemnik storitve na svojo zahtevo, v smislu člena 14 Direktive 2000/31/ES, ne glede na kraj sedeža, in katerega dejavnost je usmerjena na potrošnike, ki prebivajo v Uniji;
 - (b) „nezakonite vsebine“ pomenijo katero koli informacijo, ki ni v skladu s pravom Unije ali zakonodajo zadevne države članice;
 - (c) „uporabnik“ pomeni vsako fizično ali pravno osebo, ki je prejemnik storitev, ki jih zagotavlja ponudnik storitev gostovanja;
 - (d) „ponudnik vsebin“ pomeni uporabnika, ki je predložil informacije, ki jih ponudnik storitev gostovanja hrani ali jih je hranil na njegovo zahtevo;
 - (e) „prijava“ pomeni vsa sporočila, ki jih prijavitelj naslovi na ponudnika storitve gostovanja v zvezi z vsebinami, ki jih ponudnik storitev gostovanja hrani in za katere prijavitelj meni, da so nezakonite, ter zahteva, da jih ponudnik storitev gostovanja prostovoljno odstrani ali onemogoči dostop do njih;
 - (f) „prijavitelj“ pomeni posameznika ali subjekt, ki je ponudniku storitev gostovanja predložil prijavo;
 - (g) „zaupanja vredni prijavitelj“ pomeni posameznika ali subjekt, ki ima po mnenju ponudnika storitev gostovanja posebno strokovno znanje in pristojnosti za boj proti nezakonitim spletnim vsebinam;
 - (h) „teroristične vsebine“ pomenijo vse informacije, katerih razširjanje pomeni kazniva dejanja iz Direktive (EU) 2017/541 ali teroristična kazniva dejanja, določena v zakonodaji zadevne države članice, vključno s razširjanjem ustreznih informacij, ki jih oblikujejo teroristične skupine ali subjekti, vključeni na ustrezne sezname Unije ali Združenih narodov, ali ustreznih informacij, ki jim jih je mogoče pripisati;
 - (i) „organi kazenskega pregona“ pomenijo pristojne organe, ki jih določijo države članice v skladu z nacionalno zakonodajo za opravljanje nalog kazenskega pregona za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj v zvezi z nezakonitimi spletnimi vsebinami;
 - (j) „pristojni organi“ pomenijo pristojne organe, ki jih določijo države članice v skladu z nacionalno zakonodajo za opravljanje nalog, ki vključujejo boj proti nezakonitim spletnim vsebinam, vključno z organi pregona in upravnimi organi, ki so zadolženi za izvrševanje zakonodaje, ne glede na naravo ali poseben predmet urejanja navedene zakonodaje, ki se uporablja na nekaterih posebnih področjih;
 - (k) „obvestilo“ pomeni vsa sporočila, ki jih pristojni organ ali Europol naslovi na ponudnika storitev gostovanja v zvezi z vsebinami, ki jih ponudnik storitev gostovanja hrani, in za katere navedeni organ ali Europol meni, da so teroristične narave, ter zahteva, da jih ponudnik storitev gostovanja prostovoljno odstrani ali onemogoči dostop do njih.

POGLAVJE II

Splošna priporočila v zvezi z vsemi vrstami nezakonitih vsebin

Predložitev in obdelava prijav

5. Določiti bi bilo treba mehanizme za predložitev prijav. Ti mehanizmi bi morali biti lahko dostopni, uporabniku prijazni in omogočiti predložitev prijav po elektronski poti.
6. Ti mehanizmi bi morali omogočati in spodbujati predložitev prijav, ki so dovolj natančne in ustrezno utemeljene, da zadevnemu ponudniku gostovanja omogočijo informirano in premišljeno odločitev v zvezi z vsebinami, na katere se nanaša prijava, in zlasti o tem, ali digitalne vsebine štejejo za nezakonite in jih je treba odstraniti ali onemogočiti dostop do njih. Ti mehanizmi bi morali olajšati predložitev prijav, ki vsebujejo obrazložitev razlogov, zakaj prijavitelj meni, da gre za nezakonite vsebine, in jasno opredeljujejo mesto, kjer se te vsebine nahajajo.

7. Prijavitelji bi morali imeti možnost vključiti svoje kontaktne podatke v prijavo, vendar to ne bi smelo biti obvezno. Če se za takšno vključitev odločijo, bi bilo treba zagotoviti njihovo anonimnost v razmerju do ponudnika vsebin.
8. Če so kontaktni podatki prijavitelja ponudniku storitev gostovanja znani, bi moral ponudnik storitev gostovanja prijavitelju poslati potrdilo o prejemu ter ga brez nepotrebnega odlašanja in na sorazmeren način obvestiti o svoji odločitvi v zvezi z vsebinami, na katere se nanaša prijava.

Obveščanje ponudnikov vsebin in odgovor na prijavo

9. Če se ponudnik storitev gostovanja odloči, da bo odstranil kakršne koli vsebine, ki jih hrani, ali onemogočil dostop do njih, ker meni, da so nezakonite, ne glede na uporabljeno sredstvo za odkrivanje, prepoznavanje ali odstranitev vsebin oziroma onemogočenje dostopa do njih, in če so kontaktni podatki ponudnika vsebin ponudniku storitev gostovanja znani, bi moral biti ponudnik vsebin brez nepotrebnega odlašanja in na sorazmeren način obveščen o takšni odločitvi in razlogih zanjo ter tudi o možnostih za njeno izpodbijanje iz točke 11.
10. Vendar se točka 9 ne bi smela uporabljati, če je očitno, da so zadevne vsebine nezakonite in se nanašajo na huda kazniva dejanja, ki ogrožajo življenje ali varnost ljudi. Ponudniki storitev gostovanja poleg tega ne bi smeli zagotavljati informacij iz navedene točke, če in dokler pristojni organ tako zahteva iz razlogov javnega reda in javne varnosti ter zlasti iz razlogov preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj.
11. Ponudnikom vsebin bi ponudniki storitev gostovanja morali dati možnost izpodbijanja odločitve iz točke 9, in sicer v razumnem roku in v obliki odgovora na prijavo, ki se predloži ponudniku storitev gostovanja. Mehanizem za predložitev takšnih odgovorov na prijavo bi moral biti uporabniku prijazen in omogočati predložitev v elektronski obliki.
12. Zagotoviti bi bilo treba, da ponudniki storitev gostovanja upoštevajo vsak odgovor na prijavo, ki ga prejmejo. Kadar odgovor na prijavo vključuje razloge, na podlagi katerih ponudnik storitev gostovanja lahko šteje, da vsebine, na katere se nanaša odgovor na prijavo, niso nezakonite, bi moral svojo odločitev, da odstrani vsebine ali onemogoči dostop do njih, brez nepotrebnega odlašanja razveljaviti, kar ne posega v njegovo možnost, da določi in izvršuje pogoje izvajanja svojih storitev v skladu s pravom Unije in zakonodajo držav članic.
13. Ponudnik vsebin, ki je predložil odgovor na prijavo, in zadevni prijavitelj bi morala biti v primeru, kadar so njuni kontaktni podatki ponudniku storitev gostovanja znani, brez nepotrebnega odlašanja obveščena o odločitvi, ki jo je ponudnik storitev gostovanja sprejel v zvezi z zadevnimi vsebinami.

Alternativno reševanje sporov

14. Države članice se spodbuja, da po potrebi omogočijo alternativno reševanje sporov v zvezi z odstranitvijo nezakonitih vsebin ali onemogočanjem dostopa do njih. Taki mehanizmi za alternativno reševanje sporov bi morali biti zlahka dostopni, učinkoviti, pregledni in nepristranski ter bi morali zagotavljati, da so rešitve spora pravične in v skladu s pravom, ki se uporablja. Poskusi za alternativno reševanje takšnih sporov ne bi smeli vplivati na dostop zadevnih strank do sodišča.
15. Če so mehanizmi za alternativno reševanje sporov na voljo v zadevni državi članici, se ponudnike storitev gostovanja spodbuja, naj dovolijo njihovo uporabo.

Preglednost

16. Ponudnike storitev gostovanja bi morali spodbuditi k objavljanju jasne, lahko razumljive in dovolj podrobne razlage svoje politike glede odstranitve vsebin, ki jih hranijo, ali onemogočanja dostopa do njih, vključno z vsebinami, ki štejejo za nezakonite.
17. Ponudnike storitev gostovanja bi morali spodbuditi k objavljanju poročil o svojih dejavnostih v zvezi z odstranjevanjem vsebin, ki štejejo za nezakonite, in onemogočanjem dostopa do njih v rednih presledkih, po možnosti vsaj enkrat letno. Ta poročila bi morala zlasti vključevati informacije o obsegu in vrsti vsebin, ki so bile odstranjene, o številu prejetih prijav in odgovorov na prijave ter o času, potrebnem za ukrepanje.

Proaktivni ukrepi

18. Ponudnike storitev gostovanja bi bilo treba spodbuditi, da po potrebi sprejmejo sorazmerne in posebne proaktivne ukrepe v zvezi z nezakonitimi vsebinami. Takšni proaktivni ukrepi bi lahko vključevali uporabo avtomatiziranih sredstev za odkrivanje nezakonitih vsebin samo, kadar je to ustrezno in sorazmerno ter se zanje uporabljajo učinkoviti in ustrezni zaščitni ukrepi, zlasti zaščitni ukrepi iz točk 19 in 20.

Zaščitni ukrepi

19. Da bi se izognili odstranitvi vsebin, ki niso nezakonite, brez poseganja v možnost ponudnikov storitev gostovanja, da določijo in izvršujejo pogoje izvajanja svojih storitev v skladu s pravom Unije in zakonodajo držav članic, bi morali obstajati učinkoviti in ustrezni zaščitni ukrepi, s katerimi bi zagotovili, da ponudniki storitev gostovanja ravnajo skrbno in sorazmerno v zvezi z vsebinami, ki jih hranijo, zlasti pri obdelavi prijav in odgovorov nanje ter pri odločanju o morebitni odstranitvi vsebin, ki štejejo za nezakonite, ali onemogočanju dostopa do njih.
20. Kadar ponudniki storitev gostovanja uporabljajo avtomatizirana sredstva v zvezi z vsebinami, ki jih hranijo, bi bilo treba zagotoviti učinkovite in ustrezne zaščitne ukrepe za zagotovitev, da so odločitve, ki jih sprejmejo v zvezi s temi vsebinami, zlasti odločitve, da se vsebine, ki štejejo za nezakonite, odstranijo ali se onemogoči dostop do njih, pravilne in utemeljene. Taki zaščitni ukrepi bi morali vključevati zlasti človeški nadzor in preverjanje, kjer je to primerno, in v vsakem primeru, če je potrebna podrobna analiza zadevnih okoliščin, za ugotovitev, ali vsebine štejejo za nezakonite ali ne.

Zaščita pred zlorabo

21. Treba bi bilo sprejeti učinkovite in ustrezne ukrepe za preprečitev predložitve prijav ali odgovorov na prijave, ki so vloženi v slabi veri, ali ukrepanja v zvezi z njimi ter drugih oblik zlorabe v zvezi s priporočenimi ukrepi za boj proti nezakonitim spletnim vsebinam iz tega priporočila.

Sodelovanje med ponudniki storitev gostovanja in državami članicami

22. Države članice in ponudniki storitev gostovanja bi morali določiti kontaktne točke za zadeve v zvezi z nezakonitimi spletnimi vsebinami.
23. Določiti bi bilo treba hitre postopke za obravnavo prijav, ki jih predložijo pristojni organi.
24. Države članice se spodbujajo k vzpostavitvi pravne obveznosti za ponudnike storitev gostovanja, da za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj organe kazenskega pregona takoj obvestijo o vseh dokazih o domnevnih hudih kaznivih dejanjih, ki ogrožajo življenje ali varnost ljudi, pridobljenih v okviru svojih dejavnosti za odstranitev nezakonitih vsebin ali preprečitev dostopa do njih, v skladu z veljavnimi pravnimi zahtevami, zlasti v zvezi z varstvom osebnih podatkov, vključno z Uredbo (EU) 2016/679.

Sodelovanje med ponudniki storitev gostovanja in zaupanja vrednimi prijavitelji

25. Sodelovanje med ponudniki storitev gostovanja in zaupanja vrednimi prijavitelji bi bilo treba spodbujati. Zlasti bi bilo treba določiti hitre postopke za obravnavo prijav, ki jih predložijo zaupanja vredni prijavitelji.
26. Ponudnike storitev gostovanja bi morali spodbuditi k objavljanju jasnih in objektivnih pogojev za določanje, katere posameznike ali subjekte štejejo za zaupanja vredne prijavitelje.
27. Navedeni pogoji bi morali zagotavljati, da imajo zadevni posamezniki ali subjekti potrebno strokovno znanje in izvajajo svoje dejavnosti kot zaupanja vredni prijavitelji s skrbnostjo in na objektivni način ter spoštujejo vrednote, na katerih temelji Unija.

Sodelovanje med ponudniki storitev gostovanja

28. Ponudniki storitev gostovanja bi si morali po potrebi izmenjavati izkušnje, tehnološke rešitve in dobre prakse za boj proti nezakonitim spletnim vsebinam, in sicer med seboj ter zlasti s ponudniki storitev gostovanja, ki imajo zaradi svoje velikosti ali obsega delovanja omejene vire in strokovno znanje, tudi v okviru tekočega sodelovanja med ponudniki storitev gostovanja prek kodeksov ravnanja, memorandumov o soglasju in drugih prostovoljnih dogovorov.

POGLAVJE III**Posebna priporočila v zvezi s terorističnimi vsebinami***Splošno*

29. Posebna priporočila v zvezi s terorističnimi vsebinami, ki so določena v tem poglavju, veljajo poleg splošnih priporočil, določenih v poglavju II.
30. Ponudniki storitev gostovanja bi morali v pogojih izvajanja svojih storitev izrecno določiti, da ne bodo hranili terorističnih vsebin.
31. Ponudniki storitev gostovanja bi morali sprejeti ukrepe, ki preprečujejo hrambo terorističnih vsebin, zlasti glede obvestil, proaktivnih ukrepov in sodelovanja v skladu s točkami 32 do 40.

Predložitev in obdelava obvestil

32. Države članice bi morale zagotoviti, da imajo njihovi pristojni organi zmogljivosti in zadostna sredstva za učinkovito odkrivanje in prepoznavanje terorističnih vsebin ter predložitev obvestil zadevnim ponudnikom storitev gostovanja, zlasti prek nacionalne enote za obveščanje o sumljivih spletnih vsebinah ter v sodelovanju z enoto EU za obveščanje o sumljivih spletnih vsebinah v okviru Europola.
33. Predvideti bi bilo treba mehanizme, ki omogočajo predložitev obvestila. Določiti bi bilo treba hitre postopke za obravnavo obvestil, zlasti obvestil, ki so jih predložile nacionalne enote za obveščanje o sumljivih spletnih vsebinah in enota EU za obveščanje o sumljivih spletnih vsebinah v okviru Europola.
34. Ponudniki storitev gostovanja bi morali brez nepotrebnega odlašanja pošiljati potrditev prejema obvestila in obvestiti pristojne organe ali Europol o svojih odločitvah v zvezi z vsebinami, na katere se nanaša obvestilo, z navedbo, kdaj so bile vsebine odstranjene ali je bil dostop do njih onemogočen oziroma zakaj so se odločili, da vsebin ne odstranijo ali ne onemogočijo dostopa do njih, odvisno od konkretnega primera.
35. Ponudniki storitev gostovanja bi morali oceniti in po potrebi odstraniti vsebine, opredeljene v obvestilu, ali onemogočiti dostop njih, in sicer načeloma v roku ene ure od prejema obvestila.

Proaktivni ukrepi

36. Ponudniki storitev gostovanja bi morali sprejeti sorazmerne in posebne proaktivne ukrepe, vključno z uporabo avtomatiziranih sredstev, za odkrivanje, prepoznavanje in hitro odstranitev terorističnih vsebin ali onemogočenje dostopa do njih.
37. Ponudniki storitev gostovanja bi morali sprejeti sorazmerne in posebne proaktivne ukrepe, vključno z uporabo avtomatiziranih sredstev, da bi se ponudnikom vsebin takoj preprečila ponovna predložitev vsebin, ki so že bile odstranjene ali do katerih je bil dostop že onemogočen, ker štejejo za teroristične.

Sodelovanje

38. Da bi se preprečilo širjenje terorističnih vsebin med različnimi storitvami gostovanja, bi bilo treba ponudnike storitev gostovanja spodbujati k sodelovanju z izmenjavo in optimizacijo učinkovitih, primernih in sorazmernih tehnoloških orodij, vključno s tistimi orodji, ki omogočajo samodejno zaznavanje vsebin. Kadar je to tehnološko mogoče, bi bilo treba zajeti vse zadevne oblike, prek katerih se razširjajo teroristične vsebine. V to sodelovanje bi bilo treba vključiti zlasti ponudnike storitev gostovanja, ki imajo zaradi svoje velikosti ali obsega delovanja omejene vire in strokovno znanje.

39. Ponudnike storitev gostovanja bi bilo treba spodbujati k sprejetju potrebnih ukrepov za pravilno delovanje in izboljšanje orodij iz točke 38, zlasti z zagotavljanjem identifikatorjev, ki se nanašajo na vse vsebine, ki veljajo za teroristične, in s polnim izkoriščanjem možnosti navedenih orodij.
40. Pristojni organi in ponudniki storitev gostovanja bi morali skleniti delovne ureditve, po potrebi tudi z Europolom, glede zadev, ki se nanašajo na teroristične spletne vsebine, in sicer tudi za izboljšanje razumevanja terorističnih dejavnosti na spletu, izboljšanje mehanizmov obvestila, preprečitev nepotrebne podvajanja prizadevanj ter lažje podajanje zahtev s strani organov kazenskega pregona za namene kazenskih preiskav v zvezi s terorizmom.

POGLAVJE IV

Zagotavljanje informacij

41. Države članice bi morale v rednih časovnih presledkih in po možnosti vsake tri mesece poročati Komisiji o obvestilih, ki so jih predložili njihovi pristojni organi, in o odločitvah, ki so jih sprejeli ponudniki storitev gostovanja na podlagi teh obvestil, kakor tudi o njihovem sodelovanju s ponudniki storitev gostovanja v zvezi z bojem proti terorističnim vsebinam.
42. Da bi omogočili spremljanje učinkov tega priporočila v zvezi s terorističnimi vsebinami, bi morali ponudniki storitev gostovanja najpozneje tri mesece od datuma objave priporočila Komisiji na njeno zahtevo predložiti vse ustrezne informacije, da se omogoči takšno spremljanje. Te informacije lahko vključujejo zlasti informacije o obsegu vsebin, ki so že bile odstranjene ali do katerih je bil dostop že onemogočen, bodisi na podlagi obvestila ali prijave ali na podlagi sprejetih proaktivnih ukrepov in uporabe avtomatiziranih sredstev. Vključujejo lahko tudi število prejetih obvestil in čas, potreben za ukrepanje, ter tudi obseg vsebin, ki jih ni bilo mogoče predložiti ali ponovno predložiti na podlagi uporabe samodejnega zaznavanja vsebin in drugih tehnoloških orodij.
43. Da bi omogočili spremljanje učinkov tega priporočila v zvezi z nezakonitimi vsebinami, ki niso teroristične vsebine, bi morali države članice in ponudniki storitev gostovanja najpozneje šest mesecev po objavi priporočila Komisiji na njeno zahtevo predložiti vse pomembne informacije, da se omogoči takšno spremljanje.

V Bruslju, 1. marca 2018

Za Komisijo
Andrus ANSIP
Podpredsednik
