Rada
Európskej únie

V Bruseli 7. decembra 2018
(OR. en)

15336/18

Medziinštitucionálny spis:
2018/0331(COD)

CT 198
ENFOPOL 605
JAI 1264
COTER 175
CYBER 313
TELECOM 461
FREMP 222
AUDIO 121
DROIPEN 199
CODEC 2270

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	6. decembra 2018
Komu:	Delegácie
Č. predch. dok.:	14978/18 + COR 1
Č. dok. Kom.:	12129/18 + ADD 1-3
Predmet:	Návrh nariadenia Európskeho parlamentu a Rady o predchádzaní šíreniu teroristického obsahu online – všeobecné smerovanie

Rada sa na svojom zasadnutí 6. decembra 2018 dohodla na všeobecnom smerované uvedenom v prílohe.

Zmeny oproti návrhu Komisie sú vyznačené ***tučnou kurzívou*** v prípade doplnení a symbolom […] v prípade vypusteného textu.

PRÍLOHA

[…]

[…] Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o predchádzaní šíreniu teroristického obsahu online

[…]

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[1],

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

(1) Cieľom tohto nariadenia je zabezpečiť hladké fungovanie jednotného digitálneho trhu v otvorenej a demokratickej spoločnosti tým, že sa zabráni zneužívaniu hostingových služieb na teroristické účely. Fungovanie jednotného digitálneho trhu by sa malo zlepšiť posilnením právnej istoty pre poskytovateľov hostingových služieb, posilnením dôvery používateľov v online prostredie a posilnením záruk v súvislosti so slobodou prejavu a právom na informácie.

[1] Ú. v. EÚ C , , s. .

(2) Poskytovatelia hostingových služieb pôsobiaci na internete zohrávajú dôležitú úlohu v digitálnom hospodárstve tým, že spájajú podniky a občanov a uľahčujú verejnú diskusiu a šírenie a prijímanie informácií, názorov a myšlienok, ktoré významnou mierou prispievajú k inováciám, hospodárskemu rastu a tvorbe pracovných miest v Únii. Ich služby sú však v určitých prípadoch zneužívané tretími stranami na nezákonnú činnosť online. Osobitné obavy vyvoláva zneužívanie poskytovateľov hostingových služieb zo strany teroristických skupín a ich podporovateľov na šírenie teroristického obsahu online s cieľom rozšíriť ich posolstvo, radikalizovať a uskutočniť nábor, ako aj na uľahčenie a riadenie teroristickej činnosti.

(3) Prítomnosť teroristického obsahu na internete má vážne negatívne dôsledky pre používateľov, občanov a spoločnosť ako celok, ako aj pre poskytovateľov služieb online, ktorí sú hostiteľmi takéhoto obsahu, pretože podkopáva dôveru používateľov a poškodzuje ich obchodné modely. Vzhľadom na svoju ústrednú úlohu a technologické prostriedky a kapacity spojené so službami, ktoré poskytujú, majú poskytovatelia online služieb určité spoločenské povinnosti, pokiaľ ide o ochranu ich služieb pred zneužitím zo strany teroristov a ich pomoc pri riešení teroristického obsahu šíreného prostredníctvom ich služieb.

(4) Úsilie na úrovni Únie zamerané na boj proti teroristickému obsahu online, ktoré sa začalo v roku 2015 prostredníctvom dobrovoľnej spolupráce medzi členskými štátmi a poskytovateľmi hostingových služieb, musí byť doplnené jasným legislatívnym rámcom s cieľom ďalej znižovať prístup k teroristickému obsahu online a primerane reagovať na rýchlo sa vyvíjajúci problém. Cieľom tohto legislatívneho rámca je stavať na dobrovoľnom úsilí, ktoré bolo posilnené odporúčaním Komisie (EÚ) 2018/334[2], pričom tento legislatívny rámec je reakciou na výzvy Európskeho parlamentu, aby sa posilnili opatrenia na boj proti nezákonnému a škodlivému obsahu, a na výzvy Európskej rady, aby sa zlepšilo automatické odhaľovanie a odstraňovanie obsahu, ktorý podnecuje na teroristické činy.

[2] Odporúčanie Komisie (EÚ) 2018/334 z 1. marca 2018 o opatreniach na účinný boj proti nezákonnému obsahu na internete (Ú. v. EÚ L 63, 6.3.2018, s. 50).

(5) Uplatňovanie tohto nariadenia by nemalo mať vplyv na uplatňovanie článku 14 smernice 2000/31/ES[3]. Predovšetkým by žiadne opatrenia, ktoré prijal poskytovateľ hostingových služieb v súlade s týmto nariadením, vrátane akýchkoľvek proaktívnych opatrení, nemali samé osebe viesť k tomu, že tento poskytovateľ služieb príde o výhodu výnimky zo zodpovednosti stanovenej v uvedenom ustanovení. Toto nariadenie nemá vplyv na právomoci vnútroštátnych orgánov a súdov, pokiaľ ide o stanovenie zodpovednosti poskytovateľov hostingových služieb v osobitných prípadoch, keď nie sú splnené podmienky zakladajúce výnimku zo zodpovednosti podľa článku 14 smernice 2000/31/ES. ***Toto nariadenie sa nevzťahuje na činnosti súvisiace s národnou bezpečnosťou, keďže tá ostáva vo výlučnej zodpovednosti každého členského štátu.***

(6) V tomto nariadení sa stanovujú pravidlá na predchádzanie zneužívaniu hostingových služieb na šírenie teroristického obsahu online s cieľom zaručiť bezproblémové fungovanie vnútorného trhu, a to pri plnom rešpektovaní základných práv, ktoré sú chránené v právnom poriadku Únie, a najmä tých, ktoré sú zaručené v Charte základných práv Európskej únie.

---

[3] Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode) (Ú. v. ES L 178, 17.7.2000, s. 1).

(7) Toto nariadenie prispieva k ochrane verejnej bezpečnosti a zároveň vytvára primerané a spoľahlivé záruky na zabezpečenie ochrany dotknutých základných práv. Zahŕňa právo na rešpektovanie súkromného života a na ochranu osobných údajov, právo na účinnú súdnu ochranu, právo na slobodu prejavu vrátane slobody prijímať a rozširovať informácie, ako aj slobodu podnikania a zásadu nediskriminácie. Príslušné orgány a poskytovatelia hostingových služieb by mali prijímať len opatrenia, ktoré sú potrebné, vhodné a primerané v demokratickej spoločnosti, s prihliadnutím na osobitný význam, ktorý majú sloboda prejavu a právo na informácie, ***ako aj sloboda tlače a pluralita médií,*** ktoré sú […] […] základnými piliermi pluralistickej, demokratickej spoločnosti a jedny z hodnôt, na ktorých je Únia založená. Opatrenia, ktoré predstavujú zásah do slobody prejavu a práva na informácie, by mali byť presne zamerané v tom zmysle, že musia slúžiť na predchádzanie šíreniu teroristického obsahu, ale bez toho, aby to malo vplyv na právo prijímať a odovzdávať informácie zákonným spôsobom, a to pri zohľadnení ústrednej úlohy poskytovateľov hostingových služieb pri uľahčovaní verejnej diskusie a prijímaní a šírení faktov, názorov a myšlienok v súlade so zákonom.

(8) Právo na účinný prostriedok nápravy je zakotvené v článku 19 ZEÚ a v článku 47 Charty základných práv Európskej únie. Každá fyzická alebo právnická osoba má právo na účinný súdny prostriedok nápravy pred príslušným vnútroštátnym súdom proti ktorémukoľvek z opatrení prijatých podľa tohto nariadenia, ktoré môžu mať nepriaznivý vplyv na práva tejto osoby. Toto právo zahŕňa najmä možnosť poskytovateľov hostingových služieb a poskytovateľov obsahu účinne namietať proti príkazom na odstránenie na súde členského štátu, ktorého orgány toto rozhodnutie vydali, a ***možnosť poskytovateľov hostingových služieb namietať proti rozhodnutiu o uložení proaktívnych opatrení alebo sankcií na súde členského štátu, v ktorom sú usadení alebo v ktorom majú právneho zástupcu***.

(9) V záujme ozrejmenia opatrení, ktoré by mali prijať poskytovatelia hostingových služieb aj príslušné orgány s cieľom zabrániť šíreniu teroristického obsahu online, by sa v tomto nariadení malo stanoviť vymedzenie teroristického obsahu na preventívne účely, a to na základe vymedzenia teroristických trestných činov obsiahnutého v smernici Európskeho parlamentu a Rady (EÚ) 2017/541[4]. So zreteľom na potrebu riešiť najškodlivejšiu teroristickú propagandu online by sa do tohto vymedzenia mal zahrnúť materiál [...], ktorý nabáda na páchanie teroristických trestných činov alebo na poskytnutie pomoci pri páchaní týchto činov, resp. na ne motivuje alebo ich ospravedlňuje, […] alebo ktorý podporuje účasť na činnostiach teroristickej skupiny. [...] ***Okrem toho toto vymedzenie zahŕňa aj obsah, ktorý poskytuje usmernenia na výrobu a používanie výbušnín, strelných zbraní alebo iných zbraní, alebo škodlivých alebo nebezpečných látok, ako aj látok CBRN, či iných metód a techník vrátane výberu cieľov na účely spáchania teroristických trestných činov.*** Takýto [...] ***materiál*** zahŕňa najmä text, obrázky, zvukové záznamy a videá. Pri posudzovaní toho, či obsah predstavuje teroristický obsah v zmysle tohto nariadenia, by príslušné orgány, ako aj poskytovatelia hostingových služieb mali zohľadniť také faktory, ako je napr. povaha a znenie vyhlásení, kontext, v ktorom boli tieto vyhlásenia urobené, ako aj ich potenciál viesť k škodlivým následkom s vplyvom na bezpečnosť a ochranu osôb. Významným faktorom pri posudzovaní je skutočnosť, že materiál vyrobila teroristická organizácia alebo osoba uvedená na zozname EÚ, resp. že je materiál tejto organizácii či osobe pripísateľný alebo šírený v jej mene. Obsah, ktorý sa šíri na vzdelávacie, [...], ***protiargumentačné*** alebo výskumné účely, by mal byť primerane chránený, ***pričom by sa mala dosiahnuť spravodlivá rovnováha medzi základnými právami vrátane slobody prejavu a práva na informácie a potrebami v oblasti verejnej bezpečnosti. Ak sa šírený materiál uverejňuje na redakčnú zodpovednosť poskytovateľa obsahu, pri každom rozhodovaní o odstránení takéhoto obsahu by sa mali zohľadniť žurnalistické normy stanovené tlačovými alebo mediálnymi predpismi v súlade s právom Únie, právom na slobodu prejavu a právom na slobodu a pluralitu médií, ktoré je zakotvené v článku 11 Charty základných práv Európskej únie.*** Okrem toho by sa vyjadrovanie radikálnych, polemických alebo kontroverzných názorov vo verejnej diskusii o citlivých politických otázkach nemalo považovať za teroristický obsah.

---

[4] Smernica Európskeho parlamentu a Rady (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/475/SVV a mení rozhodnutie Rady 2005/671/SVV (Ú. v. EÚ L 88, 31.3.2017, s. 6).

(10) S cieľom zahrnúť tie online hostingové služby, kde sa šíri teroristický obsah, by sa toto nariadenie malo uplatňovať na služby informačnej spoločnosti, ktoré uchovávajú informácie a ***materiál*** poskytované príjemcom služby na jeho žiadosť a ktoré sprístupňujú tieto uchovávané informácie a ***materiál*** tretím stranám, a to bez ohľadu na to, či je táto činnosť čisto technickej, automatickej alebo pasívnej povahy. […] ***Uchovávanie obsahu pozostáva z uchovávania údajov v pamäti fyzického alebo virtuálneho servera; do rozsahu pôsobnosti pritom nepatria samotné vedenia a iné elektronické komunikačné služby v zmysle [európskeho kódexu elektronickej komunikácie] ani poskytovatelia služieb vyrovnávacej pamäte či iné služby poskytované v iných vrstvách infraštruktúry internetu, ako sú registre a registrátori, systém názvov domén (DNS) alebo pridružené služby, ako sú platobné služby alebo služby ochrany pred útokmi DDoS. Ďalej sa informácie musia ukladať na žiadosť poskytovateľa obsahu; do rozsahu pôsobnosti patria len tie služby, ktorých je poskytovateľ obsahu priamym príjemcom. Uložené informácie sú k dispozícii tretím stranám, čiže akémukoľvek tretiemu používateľovi, ktorý nie je poskytovateľom obsahu. Do rozsahu pôsobnosti nepatria interpersonálne komunikačné služby, ktoré umožňujú priamu interpersonálnu a interaktívnu výmenu informácií medzi pevne stanoveným počtom osôb, pričom osoby, ktoré komunikáciu začali alebo sa na nej zúčastňujú, určujú jej prijímateľov.*** Medzi takýchto poskytovateľov ***hostingových služieb*** patria napríklad […] platformy sociálnych médií, služby na videoprenos, služby na zdieľanie videí, obrazových a zvukových materiálov, služby na zdieľanie súborov a iné cloudové a ***úložné*** služby […]. ***Toto nariadenie sa vzťahuje na činnosti poskytovania hostingových služieb, a nie na konkrétneho poskytovateľa alebo jeho hlavnú činnosť, ktorá môže byť kombináciou hostingových služieb a iných služieb, ktoré nepatria do rozsahu pôsobnosti tohto nariadenia.***

(10a) Toto nariadenie by sa malo uplatňovať aj na poskytovateľov hostingových služieb usadených mimo Únie, ktorí však poskytujú svoje služby v rámci Únie, keďže významné množstvo poskytovateľov hostingových služieb vystavených teroristickému obsahu prostredníctvom ich služieb je usadené v tretích krajinách. Tým by sa malo zabezpečiť, aby všetky spoločnosti pôsobiace na jednotnom digitálnom trhu spĺňali rovnaké požiadavky bez ohľadu na krajinu, v ktorej sú usadené. Určenie toho, či poskytovateľ služieb ponúka služby v Únii, si vyžaduje posúdenie toho, či poskytovateľ služieb umožňuje právnickým alebo fyzickým osobám, aby využívali jeho služby v jednom členskom štáte alebo vo viacerých členských štátoch. Samotná prístupnosť webovej lokality poskytovateľa služieb, resp. jeho e-mailovej adresy a iných kontaktných údajov, v jednom alebo viacerých členských štátoch, by však nemala byť dostatočnou podmienkou na uplatňovanie tohto nariadenia.

(11) Pre určenie rozsahu pôsobnosti tohto nariadenia by malo byť relevantné kritérium podstatnej väzby s Úniou. Takáto podstatná väzba s Úniou by mala existovať v prípade, že poskytovateľ služieb má v Únii prevádzkareň, alebo ak ju nemá, v prípade existencie významného počtu používateľov v jednom alebo vo viacerých členských štátoch, alebo v prípade, že sa jeho činnosti zameriavajú na jeden alebo viacero členských štátov. Zameranie činností na jeden alebo viac členských štátov možno stanoviť na základe všetkých relevantných okolností vrátane faktorov, ako je napr. používanie jazyka alebo meny, ktoré sa všeobecne používa v danom členskom štáte, resp. na základe možnosti objednávania tovaru alebo služieb. Zameranie činností na určitý členský štát by sa mohlo odvodiť aj z dostupnosti aplikácie v príslušnom vnútroštátnom obchode s aplikáciami, z poskytovania miestnej reklamy alebo reklamy v jazyku používanom v danom členskom štáte, alebo z riešenia vzťahov so zákazníkmi, ako je napr. poskytovanie služieb zákazníkom v jazyku všeobecne používanom v danom členskom štáte. Podstatnú väzbu možno vyvodzovať aj z toho, ak poskytovateľ služieb smeruje svoje činnosti do jedného alebo viacerých členským štátov, ako je stanovené v článku 17 ods. 1 písm. c) nariadenia Európskeho parlamentu a Rady (ES) č. 1215/2012[5]. Na druhej strane, poskytovanie služby výlučne len v záujme dodržiavania zákazu diskriminácie stanoveného v nariadení Európskeho parlamentu a Rady (EÚ) 2018/302[6], sa samo osebe nemôže považovať za smerovanie činnosti do daného územia v rámci Únie, alebo zameranie sa na toto územie.

---

[5] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1215/2012 z 12. decembra 2012 o právomoci a o uznávaní a výkone rozsudkov v občianskych a obchodných veciach (Ú. v. EÚ L 351, 20.12.2012, s. 1).

[6] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/302 z 28. februára 2018 o riešení neodôvodneného geografického blokovania a iných foriem diskriminácie z dôvodu štátnej príslušnosti, miesta bydliska alebo sídla zákazníkov na vnútornom trhu, ktorým sa mení nariadenia (ES) č. 2006/2004 a (EÚ) 2017/2394 a smernica 2009/22/ (Ú. v. EÚ L 601, 2.3.2018, s. 1).

(12) Poskytovatelia hostingových služieb by mali uplatňovať určitú povinnú starostlivosť, aby sa zabránilo šíreniu teroristického obsahu v ich službách. Táto povinná starostlivosť by nemala znamenať všeobecnú povinnosť monitorovať. Povinná starostlivosť by mala zahŕňať to, že poskytovatelia hostingových služieb budú pri uplatňovaní tohto nariadenia konať dôsledne, primeraným a nediskriminačným spôsobom, pokiaľ ide o obsah, ktorý uchovávajú, najmä pri uplatňovaní svojich vlastných podmienok, s cieľom vyhnúť sa odstráneniu obsahu, ktorý nie je teroristickým **obsahom**. Odstránenie alebo znemožnenie prístupu sa musí realizovať tak, aby bola dodržaná sloboda prejavu a právo na informácie.

(13) Mali by sa zosúladiť postup a povinnosti vyplývajúce z právnych príkazov, ktorými sa požaduje, aby poskytovatelia hostingových služieb na základe posúdenia príslušnými orgánmi odstránili teroristický obsah alebo znemožnili prístup k nemu. Členské štáty by mali mať naďalej slobodu výberu, pokiaľ ide o určenie správnych orgánov, orgánov presadzovania práva alebo justičných orgánov, príslušných na plnenie tejto úlohy. So zreteľom na rýchlosť, akou sa šíri teroristický obsah v rámci služieb online, sa týmto ustanovením ukladajú poskytovateľom hostingových služieb povinnosti zabezpečiť, aby bol teroristický obsah uvedený v príkaze na odstránenie odstránený, resp. aby bol znemožnený prístup k nemu, do jednej hodiny od prijatia tohto príkazu. ***Bez toho, aby boli dotknuté požiadavky na uchovávanie údajov podľa článku 7 tohto nariadenia alebo podľa [návrhu predpisov o elektronických dôkazoch], j***e na rozhodnutí poskytovateľov hostingových služieb, či príslušný obsah odstránia alebo či k nemu znemožnia prístup používateľom v Únii. ***Malo by sa tým zabrániť prístupu alebo aspoň sťažiť prístup k obsahu, ku ktorému bol znemožnený prístup, a používatelia internetu, ktorí využívajú príslušné služby, by mali byť vážne odradení od prístupu k takémuto obsahu.***

(13a) Príkaz na odstránenie by mal zahŕňať klasifikáciu príslušného obsahu ako teroristického obsahu, ako aj dostatok informácií na lokalizáciu obsahu poskytnutím URL a akýchkoľvek ďalších informácií, ako sú napríklad snímky obrazovky príslušného obsahu. Príslušný orgán by mal na žiadosť poskytnúť dodatočné odôvodnenie, prečo sa obsah považuje za teroristický obsah. Toto odôvodnenie nemusí obsahovať citlivé informácie, ktoré by mohli ohroziť vyšetrovanie. Malo by však poskytovateľovi hostingových služieb a v konečnom dôsledku poskytovateľovi obsahu umožňovať účinné uplatnenie ich práva na súdny prostriedok nápravy.

(14) Príslušný orgán by mal doručiť príkaz na odstránenie priamo adresátovi a kontaktnému miestu prostredníctvom akéhokoľvek elektronického prostriedku, ktorý umožňuje vyhotoviť písomný záznam za takých podmienok, ktoré umožnia poskytovateľovi služieb overiť pravosť, vrátane presného dátumu a času odoslania a prijatia príkazu, napríklad prostredníctvom zabezpečeného e-mailu a platforiem alebo iných zabezpečených kanálov vrátane tých, ktoré poskytovateľ služieb poskytol v súlade s pravidlami na ochranu osobných údajov. Túto požiadavku možno splniť najmä využitím kvalifikovaných elektronických doručovacích služieb pre registrované zásielky, ako je stanovené v nariadení Európskeho parlamentu a Rady (EÚ) č. 910/2014[7].

[7] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28.8.2014, s. 73).

(15) […] ***Nahlasovací*** mechanizmus, ktorý poskytovateľov hostingových služieb upozorňuje na informácie a ***materiál***, ktoré sa môžu považovať za teroristický obsah, aby ho poskytovateľ dobrovoľne posúdil z hľadiska zlučiteľnosti s vlastnými podmienkami, ***je*** […] ***mimoriadne účinným, rýchlym a primeraným prostriedkom informovania poskytovateľov hostingových služieb o konkrétnom obsahu v rámci ich služieb*** […]. Je dôležité, aby poskytovatelia hostingových služieb posúdili takéto hlásenia prednostne a poskytli rýchlu spätnú väzbu o prijatých opatreniach. Konečné rozhodnutie o tom, či odstrániť obsah, pretože nie je v súlade s ich podmienkami, je na poskytovateľoch hostingových služieb. Pokiaľ ide o vykonávanie tohto nariadenia v súvislosti s hláseniami, mandát Europolu stanovený v nariadení (EÚ) 2016/794[8] sa nemení.

(16) Vzhľadom na rozsah a rýchlosť, ktoré sú potrebné na účinnú identifikáciu a odstránenie teroristického obsahu, sú primerané proaktívne opatrenia, a to v niektorých prípadoch aj automatické, základným prvkom pri riešení teroristického obsahu online. S cieľom znížiť dostupnosť teroristického obsahu vo svojich službách by poskytovatelia hostingových služieb mali posúdiť, či je vhodné prijať proaktívne opatrenia v závislosti od rizík a úrovne vystavenia sa teroristickým obsahom, ako aj od účinkov na práva tretích strán a na verejný záujem na šírení informácií. V dôsledku toho by mali poskytovatelia hostingových služieb určiť, aké vhodné, účinné a primerané opatrenia by mali byť zavedené. Táto požiadavka by nemala znamenať všeobecnú povinnosť monitorovať. V kontexte tohto posúdenia možno uviesť, že absencia príkazov na odstránenie a hlásení adresovaných poskytovateľovi hostingových služieb je znakom nízkeho ***rizika alebo*** nízkej úrovne vystavenia teroristickému obsahu.

---

8 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/794 z 11. mája 2016 o Agentúre Európskej únie pre spoluprácu v oblasti presadzovania práva (Europol), ktorým sa nahrádzajú a zrušujú rozhodnutia Rady 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV (Ú. v. EÚ L 135, 24.5.2016, s. 53).

(17) Poskytovatelia hostingových služieb by mali pri zavádzaní proaktívnych opatrení zabezpečiť, aby bolo zachované právo užívateľov na slobodu prejavu a právo na informácie – a to aj pokiaľ ide o právo slobodne prijímať a odovzdávať informácie. Okrem požiadaviek stanovených v právnych predpisoch vrátane právnych predpisov o ochrane osobných údajov by mali poskytovatelia hostingových služieb konať s náležitou starostlivosťou a uplatňovať záruky, najmä pokiaľ ide o manuálny dohľad a overovanie, aby sa v príslušných prípadoch vyhli akémukoľvek neúmyselnému a nesprávnemu rozhodnutiu, ktoré by viedlo k odstráneniu obsahu, ktorý by nebol teroristický. Toto má osobitný význam vtedy, keď poskytovatelia hostingových služieb využívajú na odhalenie teroristického obsahu automatizované prostriedky. Akékoľvek rozhodnutie použiť automatizované prostriedky, bez ohľadu na to, či ho prijal samotný poskytovateľ hostingových služieb, alebo sa k nemu dospelo na základe žiadosti príslušného orgánu, by sa malo posúdiť so zreteľom na spoľahlivosť príslušnej technológie a následný vplyv na základné práva.

(18) S cieľom zabezpečiť, aby poskytovatelia hostingových služieb vystavení teroristickému obsahu prijali vhodné opatrenia na zabránenie zneužitia svojich služieb, by príslušné orgány mali požiadať poskytovateľov hostingových služieb, ktorí dostali konečné príkazy na odstránenie, aby podali správu o prijatých proaktívnych opatreniach. Tieto opatrenia by mohli pozostávať z opatrení na predchádzanie opakovanému nahrávaniu teroristického obsahu, ktorý bol odstránený alebo ku ktorému bol znemožnený prístup na základe príkazu na odstránenie alebo hlásení, ktoré im boli doručené, na základe porovnania s verejnými alebo súkromnými nástrojmi obsahujúcimi známy teroristický obsah. Poskytovatelia hostingových služieb takisto môžu využívať aj spoľahlivé technické nástroje na identifikáciu nového teroristického obsahu, a to tak, že buď využijú takéto nástroje, ktoré sú dostupné na trhu, alebo tie, ktoré si sami vyvinú. Poskytovateľ služieb by mal podať správu o konkrétnych proaktívnych opatreniach, ktoré zaviedol, aby príslušný orgán mohol posúdiť, či sú opatrenia účinné a primerané a či, v prípade, že sa používajú automatizované prostriedky, poskytovateľ hostingových služieb má potrebné kapacity na manuálny dohľad a overovanie. Pri posudzovaní účinnosti a primeranosti opatrení by príslušné orgány mali zohľadniť príslušné parametre vrátane počtu príkazov na odstránenie a hlásení, ktoré boli príslušnému poskytovateľovi vydané, jeho ekonomické možnosti a vplyv jeho služby na šírenie teroristického obsahu (napríklad pri zohľadnení počtu používateľov v Únii).

(19) Na požiadanie by mal príslušný orgán nadviazať s poskytovateľom hostingových služieb dialóg o proaktívnych opatreniach, ktoré treba zaviesť. Ak je to potrebné, príslušný orgán by mal prijať vhodné, účinné a primerané proaktívne opatrenia, ak sa domnieva, že prijaté opatrenia nie sú dostatočné na krytie rizík. Rozhodnutie o uložení takýchto osobitných proaktívnych opatrení by v zásade nemalo viesť k uloženiu všeobecnej povinnosti monitorovať, ako sa stanovuje v článku 15 ods. 1 smernice 2000/31/ES. Vzhľadom na mimoriadne závažné riziká spojené so šírením teroristického obsahu by rozhodnutia prijaté príslušnými orgánmi na základe tohto nariadenia mohli mať výnimku od prístupu stanoveného v článku 15 ods. 1 smernice 2000/31/ES, pokiaľ ide o určité konkrétne, cielené opatrenia, ktorých prijatie je nevyhnutné z prvoradých dôvodov verejnej bezpečnosti. Pred prijatím takýchto rozhodnutí by príslušný orgán mal dosiahnuť spravodlivú rovnováhu medzi cieľmi verejného záujmu a príslušnými základnými právami, najmä právom na slobodu prejavu a právom na informácie, ako aj právom na slobodu podnikania, a mal by poskytnúť primerané odôvodnenie.

(20) Povinnosť poskytovateľov hostingových služieb uchovávať odstránený obsah a súvisiace údaje by mala byť stanovená na osobitné účely a mala by platiť len po nevyhnutne potrebný čas. Povinnosť uchovávania je nutné vztiahnuť aj na súvisiace údaje, a to v rozsahu, v akom by sa akékoľvek takéto údaje v dôsledku odstránenia predmetného obsahu inak stratili. Súvisiace údaje môžu zahŕňať údaje ako „údaje o predplatiteľoch“ vrátane údajov, ktoré sa týkajú najmä totožnosti poskytovateľa obsahu, ***„transakčných údajov“ a*** [...] „údajov o prístupe“, čo sú napríklad údaje poskytovateľa obsahu o dátume a čase použitia alebo o prihlásení do služby a odhlásení zo služby, spolu s IP adresou, ktorú poskytovateľovi obsahu pridelil poskytovateľ služby prístupu na internet.

(21) Povinnosť uchovať obsah na účely konania v rámci správneho alebo súdneho preskúmania je nevyhnutná a opodstatnená z hľadiska zabezpečenia účinných nápravných opatrení pre poskytovateľa obsahu, ktorého obsah bol odstránený, resp. k obsahu ktorého bol znemožnený prístup, ako aj s cieľom zabezpečiť obnovenie tohto obsahu v podobe, v akej pôvodne existoval pred tým, ako bol odstránený, a to v závislosti od výsledku postupu preskúmania. Povinnosť uchovať obsah na účely vyšetrovania a trestného stíhania je odôvodnená a nevyhnutná so zreteľom na prínos, ktorý by tento materiál mohol znamenať v záujme narušenia teroristickej činnosti, resp. jej predchádzania. V prípade, že spoločnosti odstránia určitý materiál, resp. znemožnenia prístup k nemu, najmä prostredníctvom vlastných proaktívnych opatrení, a neinformujú príslušný orgán, pretože sa domnievajú, že to nepatrí do rozsahu pôsobnosti článku 13 ods. 4 tohto nariadenia, sa môže stať, že orgány presadzovania práva nebudú mať vedomosť o existencii predmetného obsahu. Uchovanie obsahu na účely predchádzania teroristickým trestným činom a ich odhaľovania, vyšetrovania a stíhania je preto takisto odôvodnené. Na tieto účely sa požadované uchovávanie údajov obmedzuje len na údaje, pri ktorých je pravdepodobné, že súvisia s teroristickými trestnými činmi, a môžu preto prispieť k stíhaniu teroristických trestných činov alebo k predchádzaniu závažným hrozbám verejnej bezpečnosti.

(22) Aby sa zabezpečila proporcionalita, obdobie uchovávania by malo byť obmedzené na šesť mesiacov, aby poskytovatelia obsahu mali dostatočný čas na začatie procesu preskúmania a aby umožnili prístup orgánom presadzovania práva k relevantným údajom na účely vyšetrovania a stíhania teroristických trestných činov. Toto obdobie sa však na požiadanie orgánu vykonávajúceho preskúmanie môže predĺžiť o čas, ktorý je potrebný v prípade, že sa proces preskúmania po začatí neskončí do šiestich mesiacov. Toto obdobie by malo postačovať na to, aby orgány presadzovania práva mohli uchovať potrebné dôkazy v súvislosti s vyšetrovaniami a zároveň zabezpečiť rovnováhu s príslušnými základnými právami.

(23) Týmto nariadením nie sú dotknuté procesné záruky ani procesné vyšetrovacie opatrenia týkajúce sa prístupu k obsahu a súvisiacim údajom, ktoré sa uchovávajú na účely vyšetrovania a trestného stíhania teroristických trestných činov v súlade s vnútroštátnymi právnymi predpismi členských štátov a právnymi predpismi Únie.

(24) Transparentnosť politík poskytovateľov hostingových služieb v súvislosti s teroristickým obsahom je nevyhnutná na posilnenie ich zodpovednosti voči ich používateľom a na posilnenie dôvery občanov v jednotný digitálny trh. Poskytovatelia hostingových služieb, ***ktorí sú vystavení teroristickému obsahu,*** by mali uverejňovať výročné správy na účely transparentnosti obsahujúce užitočné informácie o opatreniach prijatých v súvislosti s odhaľovaním, identifikáciou a odstraňovaním teroristického obsahu, ***ak to nie je v rozpore s účelom prijímaných opatrení***.

(25) Postupy podávania sťažností predstavujú nevyhnutnú záruku pred tým, aby nedošlo v ***dôsledku opatrení prijatých podľa podmienok poskytovateľov hostingových služieb*** k chybnému odstráneniu obsahu chráneného v rámci slobody prejavu a práva na informácie. Poskytovatelia hostingových služieb by preto mali vytvoriť ľahko použiteľné mechanizmy podávania sťažností a mali by zabezpečiť, aby sa sťažnosti vybavovali bezodkladne a pri plnej transparentnosti voči poskytovateľom obsahu. Požiadavka, aby poskytovateľ hostingových služieb obnovil obsah, ak bol tento obsah odstránený omylom, nijak neovplyvňuje možnosť poskytovateľa hostingových služieb uplatniť svoje vlastné podmienky z iných dôvodov. ***Okrem toho by poskytovatelia obsahu, ktorých obsah bol odstránený na základe príkazu na odstránenie, mali mať právo na účinný prostriedok nápravy v súlade s článkom 19 ZEÚ a článkom 47 Charty základných práv Európskej únie.***

(26) ***Na všeobecnejšej úrovni si*** […]účinná právna ochrana podľa článku 19 Zmluvy o EÚ a článku 47 Charty základných práv Európskej únie vyžaduje, aby boli osoby schopné zistiť dôvody, na základe ktorých bol obsah, ktorý nahrali, odstránený, alebo na základe ktorých bol k nemu znemožnený prístup. Na tento účel by poskytovateľ hostingových služieb mal dať poskytovateľovi obsahu k dispozícii zmysluplné informácie, ktoré by umožňovali napadnúť príslušné rozhodnutie. Uvedené si však nevyhnutne nevyžaduje vydanie oznámenia poskytovateľovi obsahu. V závislosti od okolností môžu poskytovatelia hostingových služieb nahradiť obsah považovaný za teroristický správou, že tento obsah bol odstránený, resp. že prístup k tomu obsahu bol znemožnený v súlade s týmto nariadením. Na požiadanie by sa mali poskytnúť ďalšie informácie o dôvodoch, ako aj o možnostiach, ktoré má poskytovateľ obsahu, pokiaľ ide o napadnutie príslušného rozhodnutia. Ak príslušné orgány rozhodnú, že z dôvodov verejnej bezpečnosti, a to aj v kontexte vyšetrovania, sa považuje za nevhodné alebo kontraproduktívne, aby bol poskytovateľ obsahu priamo oboznámený s odstránením určitého obsahu, resp. so znemožnením prístupu k nemu, mali by o tom informovať poskytovateľa hostingových služieb.

(27) S cieľom vyhnúť sa duplicite a možným zásahom do vyšetrovaní by sa príslušné orgány mali navzájom informovať, koordinovať a spolupracovať, a v príslušných prípadoch takisto aj s Europolom, […] ***skôr ako*** vydajú príkazy na odstránenie, alebo ***keď*** zasielajú hlásenia poskytovateľom hostingových služieb. Pri rozhodovaní o vydaní príkazu na odstránenie by mal príslušný orgán náležite zohľadniť každé oznámenie o zasahovaní do vyšetrovacích záujmov (predchádzanie kompetenčným sporom). […] ***Pri rozhodovaní o vydaní príkazu na odstránenie by mal príslušný orgán náležite zohľadniť každé oznámenie o zasahovaní do vyšetrovacích záujmov (predchádzanie kompetenčným sporom). Keď príslušný orgán dostane od príslušného orgánu z iného členského štátu informácie o existujúcom príkaze na odstránenie, nemal by sa vydávať duplikát.*** Pokiaľ ide o vykonávanie ustanovení tohto nariadenia, Europol by mohol poskytovať podporu v súlade so svojim súčasným mandátom a existujúcim právnym rámcom.

(28) S cieľom zabezpečiť účinné a dostatočne koherentné vykonávanie proaktívnych opatrení by mali príslušné orgány v členských štátoch navzájom spolupracovať, pokiaľ ide o diskusie, ktoré vedú s poskytovateľmi hostingových služieb na tému určenia, vykonávania a posudzovania osobitných proaktívnych opatrení. Takáto spolupráca je takisto potrebná aj v súvislosti s prijímaním pravidiel upravujúcich sankcie, ako aj v súvislosti s uplatňovaním a presadzovaním týchto sankcií. ***Komisia by mala takúto koordináciu a spoluprácu uľahčovať.***

(29) Je nevyhnutné, aby bol príslušný orgán členského štátu, ktorý je zodpovedný za ukladanie týchto sankcií, v plnej miere informovaný o vydávaní príkazov na odstránenie a hláseniach, ako aj o následnej komunikácii medzi poskytovateľom hostingových služieb a dotknutým príslušným orgánom. Na tento účel by členské štáty mali zabezpečiť vhodné komunikačné kanály a mechanizmy, ktoré zaistia, aby sa príslušné informácie zdieľali včas.

(30) S cieľom uľahčiť rýchlu výmenu informácií medzi príslušnými orgánmi, ako aj s poskytovateľmi hostingových služieb a s cieľom zabrániť duplicite úsilia sa členské štáty […] ***nabádajú, aby*** využívali ***špecializované*** nástroje, ktoré vytvoril Europol, ako je súčasná aplikácia pre nahlasovanie internetového obsahu (IRMa) alebo následné nástroje.

(31) Vzhľadom na konkrétne závažné dôsledky určitého teroristického obsahu by poskytovatelia hostingových služieb mali bezodkladne informovať orgány v príslušnom členskom štáte alebo príslušné orgány, v ktorých majú sídlo, resp. právneho zástupcu, o existencii akýchkoľvek dôkazov o teroristických trestných činoch, o ktorých získali vedomosť. V záujme zabezpečenia proporcionality sa táto povinnosť obmedzuje len na teroristické trestné činy vymedzené v článku 3 ods. 1 smernice (EÚ) 2017/541. Táto povinnosť informovať neznamená, že poskytovatelia hostingových služieb musia aktívne vyhľadávať akékoľvek takéto dôkazy. Dotknutý členský štát je členský štát, ktorý má právomoc vo veci vyšetrovania a stíhania teroristických trestných činov podľa smernice (EÚ) 2017/541 na základe štátnej príslušnosti páchateľa alebo možnej obete trestného činu alebo cieľového miesta teroristického činu. V prípade pochybností môžu poskytovatelia hostingových služieb postúpiť informácie Europolu, ktorý by mal následne konať v súlade so svojim mandátom, a to aj tak, že postúpi tieto informácie príslušným vnútroštátnym orgánom.

(32) Príslušné orgány v členských štátoch by mali mať možnosť použiť tieto informácie na prijatie vyšetrovacích opatrení podľa vnútroštátnych právnych predpisov, resp. právnych predpisov Únie, vrátane vydania európskeho príkazu na predloženie dôkazov podľa nariadenia EÚ o európskych príkazoch na predloženie a uchovanie elektronických dôkazov v trestných veciach[9].

(33) Poskytovatelia hostingových služieb aj členské štáty by mali zriadiť kontaktné miesta, aby sa uľahčilo rýchle vybavenie príkazov na odstránenie a hlásení. Na rozdiel od právneho zástupcu slúži takéto kontaktné miesto na prevádzkové účely. Kontaktné miesto poskytovateľa hostingových služieb by malo pozostávať z akéhokoľvek vyhradeného prostriedku, ***či už interného alebo externého,*** ktorý umožní elektronické predkladanie príkazov na odstránenie a hlásení, a z technických […] ***alebo*** personálnych prostriedkov, ktoré umožnia ich rýchle spracovanie. Kontaktné miesto poskytovateľa hostingových služieb sa nemusí nachádzať v Únii a poskytovateľ hostingových služieb môže určiť existujúce kontaktné miesto, pod podmienkou, že toto kontaktné miesto je schopné plniť funkcie stanovené v tomto nariadení. S cieľom zabezpečiť odstránenie teroristického obsahu, resp. znemožnenie prístupu k nemu, do jednej hodiny od doručenia príkazu na odstránenie by mali ***poskytovatelia hostingových služieb, ktorí sú vystavení teroristickému obsahu, čoho dôkazom je doručenie príkazu na odstránenie,*** zabezpečiť, aby bolo toto kontaktné miesto dosiahnuteľné 24/7. Informácie o kontaktnom mieste by mali zahŕňať informácie o jazyku, v ktorom sa je možné na kontaktné miesto obrátiť. S cieľom uľahčiť komunikáciu medzi poskytovateľmi hostingových služieb a príslušnými orgánmi sa poskytovateľom hostingových služieb odporúča, aby umožnili komunikáciu v niektorom z úradných jazykov Únie, v ktorom sú k dispozícii ich podmienky.

(34) Keďže neexistuje všeobecná požiadavka, aby poskytovatelia hostingových služieb zabezpečili fyzickú prítomnosť na území Únie, je potrebné zabezpečiť jednoznačnosť, pokiaľ ide o otázku, pod právomoc ktorého členského štátu príslušný poskytovateľ hostingových služieb, ktorý ponúka služby v rámci Únie, patrí. Vo všeobecnosti platí, že poskytovateľ hostingových služieb patrí do právomoci toho členského štátu, v ktorom má hlavné miesto podnikateľskej činnosti alebo v ktorom určil svojho právneho zástupcu. *Z **dôvodu účinného vykonávania, naliehavosti a verejného poriadku mal však mať právomoc pre príkazy na odstránenie a hlásenia každý členský štát.***

---

[9] COM(2018) 225 final.

(35) Tí poskytovatelia hostingových služieb, ktorí nie sú usadení v Únii, by mali písomne určiť právneho zástupcu s cieľom zabezpečiť dodržiavanie a presadzovanie povinností podľa tohto nariadenia. ***Poskytovatelia hostingových služieb môžu využiť existujúceho právneho zástupcu, ak je tento právny zástupca schopný plniť funkcie stanovené v tomto nariadení.***

(36) Tento právny zástupca by mal byť právne splnomocnený konať v mene poskytovateľa hostingových služieb.

(37) Členské štáty by mali určiť príslušné orgány na účely tohto nariadenia. Požiadavka určiť príslušné orgány si nevyhnutne nevyžaduje zriadenie nových orgánov – úlohami stanovenými v tomto nariadení môžu byť poverené aj už existujúce orgány. V tomto nariadení sa vyžaduje určenie orgánov zodpovedných za vydávanie príkazov na odstránenie, hlásení a za dohľad nad proaktívnymi opatreniami a ukladanie sankcií. Je na rozhodnutí členských štátov, koľko orgánov poveria plnením týchto úloh.

(38) Sankcie sú potrebné na zabezpečenie účinného vykonávania povinností podľa tohto nariadenia zo strany poskytovateľov hostingových služieb. Členské štáty by mali prijať pravidlá týkajúce sa sankcií, ***ktoré môžu mať administratívnu alebo trestnoprávnu povahu***, pričom súčasťou týchto pravidiel môžu byť v príslušných prípadoch aj usmernenia pre ukladanie pokút. Osobitne prísne sankcie by sa mali ukladať, ak poskytovateľ hostingových služieb systematicky neodstraňuje teroristický obsah, resp. k nemu systematicky neznemožňuje prístup, do jednej hodiny od prijatia príkazu na odstránenie. Nezabezpečenie súladu v jednotlivých prípadoch by sa mohlo sankcionovať, avšak za súčasného dodržania zásady ne bis in idem a zásady proporcionality, ako aj za zabezpečenia toho, aby tieto sankcie zohľadňovali systematické zlyhanie. S cieľom zabezpečiť právnu istotu by sa v tomto nariadení malo stanoviť, v akom rozsahu môžu príslušné povinnosti podliehať sankciám. Sankcie za nedodržiavanie článku 6 by sa mali prijať len v súvislosti so záväzkami vyplývajúcimi zo žiadosti o správu podľa článku 6 ods. 2 alebo s rozhodnutím, ktorým sa ukladajú dodatočné proaktívne opatrenia podľa článku 6 ods. 4. ***Pri posudzovaní povahy porušenia pravidiel a pri rozhodovaní o uplatnení sankcií by sa mali plne dodržiavať základné práva, ako je sloboda prejavu.*** Pri určovaní toho, či by sa mali uložiť finančné sankcie, by sa mali náležite zohľadniť finančné zdroje poskytovateľa. Členské štáty zabezpečia, aby sankcie nepodporovali odstránenie obsahu, ktorý nie je teroristický.

(39) Používanie štandardizovaných formulárov uľahčuje spoluprácu a výmenu informácií medzi príslušnými orgánmi a poskytovateľmi služieb a umožňuje im rýchlejšie a účinnejšie komunikovať. Je mimoriadne dôležité zabezpečiť rýchlu akciu po prijatí príkazu na odstránenie. Formuláre znižujú náklady na preklad a prispievajú k vysokej kvalite. Formuláre odpovedí by takisto mali umožňovať štandardizovanú výmenu informácií, a to bude osobitne dôležité v prípadoch, keď poskytovatelia služieb nie sú schopní splniť uloženú povinnosť. Autentifikované kanály na predkladanie písomností môžu zaručiť pravosť príkazu na odstránenie vrátane presnosti dátumu a času jeho odoslania a prijatia.

(40) S cieľom umožniť, aby v prípade potreby bolo možné rýchlo zmeniť obsah formulárov, ktoré sa majú používať na účely tohto nariadenia, by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 Zmluvy o fungovaní Európskej únie, pokiaľ ide o zmenu príloh I, II a III k tomuto nariadeniu. S cieľom zohľadniť vývoj v oblasti technológií a súvisiaceho právneho rámca by Komisia mala byť splnomocnená aj na prijatie delegovaných aktov na doplnenie tohto nariadenia o technické požiadavky na elektronické prostriedky, ktoré majú príslušné orgány používať na prenos príkazov na odstránenie. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni expertov, a aby tieto konzultácie viedla v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva[10]. Predovšetkým v záujme zabezpečenia rovnakého zastúpenia pri príprave delegovaných aktov sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako expertom z členských štátov a experti Európskeho parlamentu a Rady majú systematicky prístup na zasadnutia expertných skupín Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.

(41) Členské štáty by mali zhromažďovať informácie o vykonávaní právnych predpisov. ***Členské štáty môžu využiť správy, ktoré predložili poskytovatelia hostingových služieb na účely transparentnosti, a doplniť ich v prípade potreby podrobnejšími informáciami. Na*** účely hodnotenia právnych predpisov by sa mal vypracovať podrobný program monitorovania výstupov, výsledkov a vplyvov tohto nariadenia.

---

10 Ú. v. EÚ L 123, 12.5.2016, s. 1.

(42) Na základe zistení a záverov v správe o vykonávaní a výsledku monitorovania by Komisia mala vykonať hodnotenie tohto nariadenia najskôr tri roky po nadobudnutí jeho účinnosti. Hodnotenie by malo vychádzať z piatich kritérií efektívnosti, účinnosti, relevantnosti, súdržnosti a pridanej hodnoty EÚ. V rámci tohto hodnotenia sa posúdi fungovanie rôznych operačných a technických opatrení stanovených v tomto nariadení vrátane účinnosti opatrení na posilnenie odhaľovania, identifikácie a odstraňovania teroristického obsahu, účinnosti ochranných mechanizmov, ako aj vplyvov na potenciálne dotknuté práva a záujmy tretích strán vrátane preskúmania požiadavky informovať poskytovateľov obsahu.

(43) Keďže ciele tohto nariadenia, a to zabezpečenie hladkého fungovania jednotného digitálneho trhu prostredníctvom predchádzania šíreniu teroristického obsahu online, nemožno uspokojivo dosiahnuť na úrovni členských štátov, ale z dôvodu rozsahu a účinkov obmedzenia je možno ho lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec toho, čo je nevyhnutné na dosiahnutie tohto cieľa,

PRIJALI TOTO NARIADENIE:

ODDIEL I
VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy a rozsah pôsobnosti

1. V tomto nariadení sa stanovujú jednotné pravidlá na predchádzanie zneužívaniu hostingových služieb na šírenie teroristického obsahu online. Stanovujú sa v ňom najmä:

   (a) pravidlá týkajúce sa povinnej starostlivosti, ktoré majú uplatňovať poskytovatelia hostingových služieb s cieľom zabrániť šíreniu teroristického obsahu prostredníctvom ich služieb a v prípade potreby zabezpečiť jeho rýchle odstránenie;

   (b) súbor opatrení, ktoré majú členské štáty zaviesť s cieľom identifikovať teroristický obsah, umožniť jeho rýchle odstránenie zo strany poskytovateľov hostingových služieb a uľahčiť spoluprácu s príslušnými orgánmi v iných členských štátoch, poskytovateľmi hostingových služieb a v prípade potreby príslušnými orgánmi Únie.

2. Toto nariadenie sa uplatňuje na poskytovateľov hostingových služieb, ktorí ponúkajú služby v Únii, bez ohľadu na ich hlavné miesto podnikateľskej činnosti.

3. ***Týmto nariadením nie je dotknutá povinnosť dodržiavať základné práva a základné právne zásady zakotvené v článku 6 Zmluvy o Európskej únii.***

Článok 2

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

(1) „poskytovateľ hostingových služieb“ je poskytovateľ služieb informačnej spoločnosti, ktoré pozostávajú z uchovávania informácií poskytnutých poskytovateľom obsahu a na jeho žiadosť a zo sprístupňovania uchovávaných informácií tretím stranám;

(2) „poskytovateľ obsahu“ je používateľ, ktorý poskytol informácie, ktoré na jeho žiadosť uchováva, resp. uchoval, poskytovateľ hostingových služieb;

(3) „ponúkať služby v Únii“ je: umožňovať právnickým alebo fyzickým osobám v jednom alebo vo viacerých členských štátoch využívať služby poskytovateľa hostingových služieb, ktorý má podstatnú väzbu na tento členský štát alebo tieto členské štáty, akou je napríklad usadenie poskytovateľa hostingových služieb v Únii;

V prípade neexistencie takéhoto usadenia sa posúdenie podstatnej väzby zakladá na konkrétnych skutkových kritériách, ako je

(a) značný počet používateľov v jednom alebo vo viacerých členských štátoch;

(b) **alebo** zameranie činností na jeden alebo viac členských štátov;

(4) „teroristické trestné činy“ sú ***jedným z úmyselných činov uvedených*** [...] v článku 3 ods. 1 smernice (EÚ) 2017/541;

(5) „teroristický obsah“ je […] ***materiál, ktorý môže prispievať k páchaniu úmyselných činov uvedených v článku 3 ods. 1 písm. a) až i) smernice 2017/541 prostredníctvom***:

aa) vyhrážania sa spáchaním teroristického činu;

(a) podnecovania na spáchanie teroristických trestných činov alebo ich obhajovania, […] ***napríklad*** […] ***ich glorifikáciou***, v dôsledku čoho vzniká nebezpečenstvo spáchania týchto činov;

(b) ***navádzania osôb alebo skupiny osôb na spáchanie*** […] teroristických trestných činov ***alebo*** […] na prispievanie k nim;

(c) propagácie činností teroristickej skupiny, a to najmä ***navádzaním osôb alebo skupiny osôb na*** […] účasť […] na trestných činnostiach teroristickej skupiny v zmysle článku 2 ods. 3 smernice (EÚ) 2017/541 alebo na podporu týchto činností;

usmerňovanie v oblasti metód alebo techník na účely páchania teroristických trestných činov;

(6) „šírenie teroristického obsahu“ je sprístupnenie teroristického obsahu tretím stranám prostredníctvom služieb poskytovateľov hostingových služieb;

(7) „podmienky“ sú všetky podmienky a ustanovenia bez ohľadu na ich názov alebo formu, ktorými sa riadi zmluvný vzťah medzi poskytovateľom hostingových služieb a jeho používateľmi;

(8) „hlásenie“ je oznámenie vydané príslušným orgánom alebo prípadne príslušným subjektom Únie poskytovateľovi hostingových služieb o informáciách, ktoré možno považovať za teroristický obsah, aby poskytovateľ mohol dobrovoľne posúdiť ich zlučiteľnosť so svojimi vlastnými podmienkami zameranými na predchádzanie šíreniu teroristického obsahu;

(9) „hlavné miesto podnikateľskej činnosti“ je ústredie alebo sídlo, kde sa vykonávajú hlavné finančné operácie a prevádzková kontrola v ***Únii***.

ODDIEL II

Opatrenia na predchádzanie šíreniu teroristického obsahu online

Článok 3

Povinná starostlivosť

1. Poskytovatelia hostingových služieb prijmú vhodné, zmysluplné a primerané opatrenia v súlade s týmto nariadením proti šíreniu teroristického obsahu a na ochranu používateľov pred teroristickým obsahom. V tejto súvislosti musia konať dôsledne, primerane a nediskriminačne a s náležitým ohľadom na základné práva používateľov, pričom zohľadnia základný význam slobody prejavu a práva na informácie v otvorenej a demokratickej spoločnosti.

2. Poskytovatelia hostingových služieb zahrnú do svojich podmienok ***ustanovenia o tom, že nebudú uchovávať teroristický obsah***, a uplatňujú ustanovenia na predchádzanie šíreniu teroristického obsahu.

Článok 4

Príkazy na odstránenie

1. Príslušný orgán má právomoc vydať […] ***príkaz na odstránenie***, ktorým sa od poskytovateľa hostingových služieb vyžaduje, aby odstránil teroristický obsah alebo znemožnil prístup k nemu.

2. Poskytovatelia hostingových služieb odstránia teroristický obsah alebo znemožnia prístup k nemu do jednej hodiny od prijatia príkazu na odstránenie.

3. Príkazy na odstránenie obsahujú v súlade so vzorom uvedeným v prílohe I tieto prvky:

   (a) identifikáciu príslušného orgánu, ktorý vydal príkaz na odstránenie, a autentifikáciu príkazu na odstránenie príslušným orgánom; […] ***posúdenie obsahu*** prinajmenšom vo forme odkazu na ***príslušné*** kategórie teroristického obsahu uvedené v článku 2 ods. 5;

(b) jednotný lokátor zdrojov (ďalej len „URL“) a v prípade potreby aj ďalšie informácie umožňujúce identifikáciu uvedeného obsahu;

(c) odkaz na toto nariadenie ako právny základ tohto príkazu na odstránenie;

(d) dátum a časovú pečiatku vydaného príkazu na odstránenie;

(e) informácie o prostriedkoch nápravy, ktoré má k dispozícii poskytovateľ hostingových služieb a ktoré má k dispozícii poskytovateľ obsahu;

(f) v príslušných prípadoch aj rozhodnutie o nezverejnení informácie o odstránení teroristického obsahu alebo o znemožnení prístupu k nemu podľa článku 11.

4. Na žiadosť poskytovateľa hostingových služieb alebo poskytovateľa obsahu poskytne príslušný orgán […] ***doplňujúce*** odôvodnenie, v ***ktorom vysvetlí, prečo sa obsah považuje za teroristický obsah,*** a to bez toho, aby bola dotknutá povinnosť poskytovateľa hostingových služieb splniť príkaz na odstránenie v lehote stanovenej v odseku 2.

5. Príslušné orgány adresujú príkazy na odstránenie hlavnému miestu podnikateľskej činnosti poskytovateľa hostingových služieb, resp. právnemu zástupcovi určenému poskytovateľom hostingových služieb podľa článku 16, a postúpia ich kontaktnému miestu uvedenému v článku 14 ods. 1. Tieto príkazy sa zasielajú elektronickými prostriedkami, ktoré umožňujú vyhotovenie písomného záznamu za podmienok umožňujúcich autentifikáciu odosielateľa, ako aj presného dátumu a času odoslania a prijatia príkazu.

6. Poskytovatelia hostingových služieb ***bez zbytočného odkladu*** […] potvrdia prijatie a […] informujú príslušný orgán o odstránení teroristického obsahu alebo o znemožnení prístupu k nemu, pričom uvedú najmä čas, kedy sa tak stalo, a to prostredníctvom vzoru uvedeného v prílohe II.

7. Ak poskytovateľ hostingových služieb nemôže splniť príkaz na odstránenie z dôvodu vyššej moci alebo faktickej nemožnosti vykonať ho, ktorú poskytovateľovi hostingových služieb nemožno pripísať na zodpovednosť, bez zbytočného odkladu informuje príslušný orgán a vysvetlí dôvody, pričom použije vzor stanovený v prílohe III. Lehota uvedená v odseku 2 sa začne uplatňovať, hneď ako pominú uvedené dôvody.

8. Ak poskytovateľ hostingových služieb nemôže splniť príkaz na odstránenie, pretože príkaz na odstránenie obsahuje zjavné chyby alebo neobsahuje dostatočné informácie na vykonanie tohto príkazu, bez zbytočného odkladu informuje príslušný orgán a požiada o ozrejmenie, pričom použije vzor stanovený v prílohe III. Lehota uvedená v odseku 2 sa začne uplatňovať, hneď ako sa poskytne ozrejmenie.

9. Po tom, ako sa príkaz na odstránenie stane konečným, príslušný orgán, ktorý ho vydal, informuje príslušný orgán dohľadu nad vykonávaním proaktívnych opatrení uvedený v článku 17 ods. 1 písm. c). Rozhodnutie o odstránení sa stane konečným, ak nebolo podané odvolanie v lehote podľa platného vnútroštátneho práva, resp. keď bolo toto rozhodnutie po odvolaní potvrdené.

Článok 4a

Konzultačný postup pre príkazy na odstránenie

1. Vydávajúci orgán predloží kópiu príkazu na odstránenie príslušnému orgánu v zmysle článku 17 ods. 1 písm. a) členského štátu, v ktorom sa nachádza hlavné miesto podnikateľskej činnosti poskytovateľa hostingových služieb, vtedy, keď tento príkaz zasiela poskytovateľovi hostingových služieb v súlade s článkom 4 ods. 5.

2. Ak má príslušný orgán členského štátu, v ktorom sa nachádza hlavné miesto podnikateľskej činnosti poskytovateľa hostingových služieb, opodstatnené dôvody domnievať sa, že príkaz na odstránenie môže ovplyvniť základné záujmy tohto členského štátu, informuje o tom vydávajúci príslušný orgán.

3. Vydávajúci orgán vezme tieto okolnosti do úvahy a v prípade potreby príkaz na odstránenie stiahne alebo upraví.

Článok 5

Hlásenia

1. Príslušný orgán alebo príslušný subjekt Únie môže zaslať poskytovateľovi hostingových služieb hlásenie.

2. Poskytovatelia hostingových služieb zavedú prevádzkové a technické opatrenia na uľahčenie rýchleho posúdenia obsahu, ktorý zaslali príslušné orgány, resp. v príslušných prípadoch príslušné subjekty Únie na účely dobrovoľného zváženia tohto obsahu.

3. Hlásenia musia byť adresované hlavnému miestu podnikateľskej činnosti poskytovateľa hostingových služieb, resp. právnemu zástupcovi určenému poskytovateľom hostingových služieb podľa článku 16 a postúpia sa kontaktnému miestu uvedenému v článku 14 ods. 1. Tieto hlásenia sa musia zasielať elektronickými prostriedkami.

4. Hlásenie musí obsahovať dostatočné […] informácie […] o dôvodoch, prečo sa určitý obsah považuje za teroristický obsah, ***pričom sa v ňom uvádza URL*** a v prípade potreby aj ďalšie informácie umožňujúce identifikáciu uvedeného teroristického obsahu.

5. Poskytovateľ hostingových služieb prednostne posúdi obsah uvedený v hlásení v kontexte svojich podmienok a rozhodne, či tento obsah odstráni alebo znemožní prístup k nemu.

6. Poskytovateľ hostingových služieb ***bez zbytočného odkladu*** […] informuje príslušný orgán alebo príslušný subjekt Únie o výsledku posúdenia a čase prijatia akéhokoľvek opatrenia na základe tohto hlásenia.

7. Ak sa poskytovateľ hostingových služieb domnieva, že hlásenie neobsahuje dostatok informácií na posúdenie uvedeného obsahu, bezodkladne o tom informuje príslušné orgány alebo príslušný subjekt Únie, pričom uvedie, aké ďalšie informácie alebo vysvetlenia sú potrebné.

Článok 6

Proaktívne opatrenia

1. Poskytovatelia hostingových služieb […] prijmú v ***závislosti od rizika a úrovne vystavenia teroristickému obsahu*** proaktívne opatrenia na ochranu svojich služieb pred šírením teroristického obsahu. Opatrenia musia byť účinné a primerané, pričom musia zohľadňovať riziko a úroveň vystavenia teroristickému obsahu, základné práva používateľov a zásadný význam slobody prejavu a práva na informácie v otvorenej a demokratickej spoločnosti.

2. Ak bol príslušný orgán uvedený v článku 17 ods. 1 písm. c) informovaný podľa článku 4 ods. 9, požiada poskytovateľa hostingových služieb, aby do troch mesiacov od prijatia žiadosti a potom aspoň raz ročne predložil správu o konkrétnych proaktívnych opatreniach, ktoré prijal, a to aj pomocou automatizovaných nástrojov, s cieľom:

   (a) […] ***účinne riešiť opätovné zverejnenie*** […] obsahu, ktorý bol predtým odstránený, resp. ku ktorému bol znemožnený prístup, pretože sa považuje za teroristický obsah;

   (b) odhaliť, identifikovať a promptne odstrániť alebo znemožniť prístup k teroristickému obsahu.

   Takáto žiadosť sa zašle hlavnému miestu podnikateľskej činnosti poskytovateľa hostingových služieb, resp. právnemu zástupcovi určenému poskytovateľom hostingových služieb.

   Správy budú obsahovať všetky relevantné informácie, ktoré príslušnému orgánu uvedenému v článku 17 ods. 1 písm. c) umožnia posúdiť, či sú proaktívne opatrenia účinné a primerané, vrátane hodnotenia fungovania všetkých používaných automatizovaných nástrojov, ako aj použitých mechanizmov manuálneho dohľadu a overovania.

3. Ak sa príslušný orgán uvedený v článku 17 ods. 1 písm. c) domnieva, že proaktívne opatrenia prijaté a oznámené podľa odseku 2 sú nedostatočné na zmiernenie a riadenie rizika a úrovne vystavenia sa teroristickému obsahu, môže poskytovateľa hostingových služieb požiadať, aby prijal ďalšie osobitné dodatočné proaktívne opatrenia. Na tento účel poskytovateľ hostingových služieb spolupracuje s príslušným orgánom uvedeným v článku 17 ods. 1 písm. c) s cieľom určiť konkrétne opatrenia, ktoré má poskytovateľ hostingových služieb zaviesť, pričom sa stanovia kľúčové ciele a kritériá, ako aj harmonogramy ich implementácie.

4. Ak do troch mesiacov od žiadosti podľa odseku 3 nemožno dospieť k žiadnej dohode, príslušný orgán uvedený v článku 17 ods. 1 písm. c) môže vydať rozhodnutie o uložení osobitných dodatočných nevyhnutných a primeraných proaktívnych opatrení. V rozhodnutí sa zohľadnia najmä ekonomické možnosti poskytovateľa hostingových služieb a účinok takýchto opatrení na základné práva používateľov, ako aj zásadný význam slobody prejavu a práva na informácie. ***Je na uvážení príslušného orgánu uvedeného v článku 17 ods. 1 písm. c), aby rozhodol o povahe a rozsahu proaktívnych opatrení v súlade s cieľmi tohto nariadenia.*** Takéto rozhodnutie sa zašle hlavnému miestu podnikateľskej činnosti poskytovateľa hostingových služieb, resp. právnemu zástupcovi určenému poskytovateľom hostingových služieb. Poskytovateľ hostingových služieb pravidelne informuje príslušný orgán uvedený v článku 17 ods. 1 písm. c) o vykonávaní týchto opatrení.

5. Poskytovateľ hostingových služieb môže kedykoľvek požiadať príslušný orgán uvedený v článku 17 ods. 1 písm. c) o preskúmanie a v prípade potreby o zrušenie žiadosti alebo rozhodnutia podľa odsekov 2, 3 a 4. Príslušný orgán poskytne odôvodnené rozhodnutie v primeranej lehote po doručení žiadosti poskytovateľa hostingových služieb.

Článok 7

Uchovávanie obsahu a súvisiacich údajov

1. Poskytovatelia hostingových služieb uchovávajú teroristický obsah, ktorý bol odstránený alebo ku ktorému bol znemožnený prístup v dôsledku rozhodnutia o odstránení, hlásenia alebo proaktívnych opatrení podľa článkov 4, 5 a 6, a súvisiace údaje odstránené v dôsledku odstránenia teroristického obsahu, […] ktoré sú potrebné na:

   (a) konania o správnom alebo súdnom preskúmaní;

   (b) predchádzanie teroristickým trestným činom, ich odhaľovanie, vyšetrovanie a stíhanie.

2. Teroristický obsah a súvisiace údaje uvedené v odseku 1 sa uchovávajú šesť mesiacov. Teroristický obsah sa na žiadosť príslušného orgánu alebo súdu uchováva počas dlhšieho obdobia, ak je to potrebné na účely prebiehajúceho konania o správnom alebo súdnom preskúmaní podľa odseku 1 písm. a).

3. Poskytovatelia hostingových služieb zabezpečia, aby sa na teroristický obsah a súvisiace údaje uchovávané podľa odsekov 1 a 2 vzťahovali primerané technické a organizačné záruky.

   Týmito technickými a organizačnými zárukami sa zabezpečí, aby uchovávaný teroristický obsah a súvisiace údaje boli prístupné a spracúvané len na účely uvedené v odseku 1 a aby bola zabezpečená vysoká úroveň bezpečnosti dotknutých osobných údajov. Poskytovatelia hostingových služieb v prípade potreby preskúmajú a aktualizujú tieto záruky.

ODDIEL III
ZÁRUKY A ZODPOVEDNOSŤ

Článok 8

Požiadavky súvisiace s transparentnosťou

1. Poskytovatelia hostingových služieb stanovia vo svojich podmienkach vlastnú politiku predchádzania šíreniu teroristického obsahu vrátane prípadného zmysluplného vysvetlenia fungovania proaktívnych opatrení, ako aj používania automatizovaných nástrojov.

2. Poskytovatelia hostingových služieb […] ***vystavení teroristickému obsahu*** uverejnia výročné správy na účely transparentnosti o opatreniach prijatých proti šíreniu teroristického obsahu.

3. Správy na účely transparentnosti obsahujú aspoň tieto informácie:

   (a) informácie o opatreniach poskytovateľa hostingových služieb v súvislosti s odhaľovaním, identifikáciou a odstraňovaním teroristického obsahu;

   (b) informácie o opatreniach poskytovateľa hostingových služieb na účely ***účinného riešenia*** […] ***opätovného zverejnenia*** obsahu, ktorý bol predtým odstránený, resp. ku ktorému bol znemožnený prístup, pretože sa považoval za teroristický obsah;

   (c) počet odstráneného teroristického obsahu, resp. teroristického obsahu, ku ktorému bol znemožnený prístup, na základe príkazov na odstránenie, hlásení alebo proaktívnych opatrení;

   (d) prehľad a výsledky postupov podávania sťažností.

Článok 9

Záruky týkajúce sa využívania a vykonávania proaktívnych opatrení

1. Ak poskytovatelia hostingových služieb používajú automatizované nástroje podľa tohto nariadenia v súvislosti s obsahom, ktorý uchovávajú, musia poskytnúť účinné a primerané záruky na zabezpečenie toho, aby rozhodnutia prijaté v súvislosti s týmto obsahom, a to najmä rozhodnutia o odstránení alebo o znemožnení prístupu k obsahu, ktorý sa považuje za teroristický, boli presné a dobre podložené.

2. Záruky zahŕňajú najmä manuálny dohľad a prípadne overovanie, a to v každom prípade vtedy, ak sa vyžaduje podrobné posúdenie príslušného obsahu s cieľom určiť, či sa má považovať za teroristický, alebo nie.

Článok 10

Mechanizmy podávania sťažností

1. Poskytovatelia hostingových služieb zavedú účinné a prístupné mechanizmy umožňujúce poskytovateľom obsahu, ktorých obsah bol odstránený, resp. ku ktorému bol znemožnený prístup v dôsledku hlásenia podľa článku 5 alebo proaktívnych opatrení podľa článku 6, podať sťažnosť voči konaniu poskytovateľa hostingových služieb s cieľom opätovného sprístupnenia obsahu.

2. Poskytovatelia hostingových služieb bezodkladne preskúmajú každú prijatú sťažnosť a bez zbytočného odkladu opätovne sprístupnia obsah, ak odstránenie alebo znemožnenie prístupu bolo neodôvodnené. O výsledku preskúmania informujú sťažovateľa.

Článok 11

Informácie pre poskytovateľov obsahu

1. Ak poskytovatelia hostingových služieb odstránili teroristický obsah alebo k nemu znemožnili prístup, sprístupnia poskytovateľovi obsahu informácie o odstránení teroristického obsahu alebo o znemožnení prístupu k nemu.

2. Poskytovateľ hostingových služieb na žiadosť poskytovateľa obsahu informuje poskytovateľa obsahu o dôvodoch odstránenia alebo znemožnenia prístupu a o možnostiach napadnutia predmetného rozhodnutia.

3. Povinnosť podľa odsekov 1 a 2 sa neuplatňuje, ak príslušný orgán rozhodne, že z dôvodov verejnej bezpečnosti, ako je napr. predchádzanie teroristickým trestným činom, ich vyšetrovanie, odhaľovanie a stíhanie, by nemalo dôjsť k zverejneniu, a to tak dlho, ako je to potrebné, avšak […] nie viac ako […] ***šesť*** týždňov od prijatia predmetného rozhodnutia. ***Ak je to opodstatnené, táto lehota sa môže raz predĺžiť o ďalších šesť týždňov.*** V takom prípade poskytovateľ hostingových služieb nezverejní žiadne informácie o odstránení teroristického obsahu alebo o znemožnení prístupu k nemu.

ODDIEL IV

Spolupráca medzi príslušnými orgánmi, subjektmi Únie a poskytovateľmi hostingových služieb

Článok 12

Kapacity príslušných orgánov

Členské štáty zabezpečia, aby ich príslušné orgány mali potrebné kapacity a dostatočné zdroje na dosiahnutie cieľov a plnenie svojich povinností podľa tohto nariadenia.

Článok 13

*Spolupráca medzi poskytovateľmi hostingových služieb, príslušnými orgánmi a v prípade potreby s […]****príslušnými*** *subjektmi Únie*

1. Príslušné orgány v členských štátoch sa navzájom informujú, koordinujú a spolupracujú, a to v prípade potreby aj s […] ***príslušnými*** subjektmi Únie, ako je napr. Europol, pokiaľ ide o príkazy na odstránenie a hlásenia, aby sa predišlo duplicite, posilnila sa koordinácia a aby sa predišlo zásahom do vyšetrovaní v rôznych členských štátoch.

2. Príslušné orgány v členských štátoch informujú príslušný orgán uvedený v článku 17 ods. 1 písm. c) a d), koordinujú a spolupracujú s ním, pokiaľ ide o opatrenia prijaté podľa článku 6 a opatrenia na presadzovanie právnych predpisov podľa článku 18. Členské štáty zabezpečia, aby mal príslušný orgán uvedený v článku 17 ods. 1 písm. c) a d) všetky príslušné informácie. Na tento účel členské štáty zabezpečia vhodné komunikačné kanály alebo mechanizmy, ktoré zaistia, aby sa príslušné informácie zdieľali včas.

3. ***V zaujme účinného vykonávania tohto nariadenia, ako aj zabránenia duplicite*** sa členské štáty a poskytovatelia hostingových služieb môžu rozhodnúť, že využijú špecializované nástroje vrátane […] nástrojov vytvorených […] ***príslušnými*** subjektmi Únie, ako je Europol, s cieľom uľahčiť najmä:

(a) spracovanie a spätnú väzbu v súvislosti s príkazmi na odstránenie podľa článku 4;

(b) spracovanie a spätnú väzbu v súvislosti s hláseniami podľa článku 5;

(c) spoluprácu s cieľom identifikovať a vykonávať proaktívne opatrenia podľa článku 6.

4. Ak sa poskytovatelia hostingových služieb dozvedia o akýchkoľvek dôkazoch o teroristických trestných činoch, […] bezodkladne informujú orgány zodpovedné za vyšetrovanie a stíhanie trestných činov v dotknutom členskom štáte ***alebo štátoch*** [...]. ***Ak nie je možné identifikovať dotknutý členský štát alebo štáty,*** […] poskytovatelia hostingových služieb ***informujú kontaktné miesto v zmysle článku 14 ods. 3 v členskom štáte, v ktorom majú hlavné miesto podnikateľskej činnosti alebo právneho zástupcu, pričom*** tieto informácie zašlú aj Europolu, aby podnikol ďalšie vhodné kroky.

Článok 14

Kontaktné miesta

1. Poskytovatelia hostingových služieb vytvoria kontaktné miesto na prijímanie príkazov na odstránenie a hlásení elektronickými prostriedkami a zabezpečia ich rýchle spracovanie podľa článkov 4 a 5. Zabezpečia, aby boli tieto informácie verejne prístupné.

2. V informáciách podľa odseku 1 sa uvedie úradný jazyk alebo jazyky Únie uvedené v nariadení č. 1/58, v ktorých sa je možné na kontaktné miesto obrátiť a v ktorých sa bude uskutočňovať ďalšia komunikácia v súvislosti s príkazmi na odstránenie a hláseniami podľa článkov 4 a 5. Medzi tieto jazyky bude patriť aspoň jeden z úradných jazykov členského štátu, v ktorom má poskytovateľ hostingových služieb svoje hlavné miesto podnikateľskej činnosti alebo v ktorom má sídlo alebo pobyt jeho zákonný zástupca podľa článku 16.

3. Členské štáty zriadia kontaktné miesto na vybavovanie žiadostí o ozrejmenie a spätnú väzbu v súvislosti s príkazmi na odstránenie a hláseniami, ktoré vydali. Informácie o kontaktnom mieste sa sprístupnia verejnosti.

ODDIEL V
VYKONÁVANIE A PRESADZOVANIE

Článok 15

Súdna právomoc

1. Právomoc na účely článkov 6, 18 a 21 má členský štát, v ktorom sa nachádza hlavné miesto podnikateľskej činnosti poskytovateľa hostingových služieb. Poskytovateľ hostingových služieb, ktorý nemá svoje hlavné miesto podnikateľskej činnosti v jednom z členských štátov, sa považuje za poskytovateľa v právomoci členského štátu, v ktorom má sídlo alebo pobyt právny zástupca uvedený v článku 16. ***Každý členský štát má právomoc na účely článkov 4 a 5 bez ohľadu na to, kde má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti alebo kde určil právneho zástupcu.***

2. Ak poskytovateľ hostingových služieb neurčí právneho zástupcu, majú právomoc všetky členské štáty. ***Ak sa členský štát rozhodne vykonávať právomoc, informuje o tom všetky ostatné členské štáty.***

[…] […]

[...]Článok 16

Právny zástupca

1. Poskytovateľ hostingových služieb, ktorý nemá v Únii prevádzkareň, ale ponúka služby v Únii, písomne určí právnickú alebo fyzickú osobu ako svojho právneho zástupcu v Únii na prijímanie, dodržiavanie a presadzovanie príkazov na odstránenie, hlásení, žiadostí a rozhodnutí vydaných príslušnými orgánmi na základe tohto nariadenia. Tento právny zástupca musí mať pobyt alebo sídlo v jednom z členských štátov, v ktorých poskytovateľ hostingových služieb ponúka služby.

2. Poskytovateľ hostingových služieb poverí právneho zástupcu prijímaním, dodržiavaním a presadzovaním príkazov na odstránenie, hlásení, žiadostí a rozhodnutí uvedených v odseku 1 v mene dotknutého poskytovateľa hostingových služieb. Poskytovatelia hostingových služieb udelia svojmu právnemu zástupcovi potrebné právomoci a zdroje, aby mohol spolupracovať s príslušnými orgánmi a dodržiavať tieto rozhodnutia a príkazy.

3. Určený právny zástupca môže niesť zodpovednosť za nedodržanie povinností podľa tohto nariadenia bez toho, aby bola dotknutá zodpovednosť a právne kroky uplatniteľné voči poskytovateľovi hostingových služieb.

4. Poskytovateľ hostingových služieb oznámi určenie právneho zástupcu príslušnému orgánu uvedenému v článku 17 ods. 1 písm. d) v členskom štáte, v ktorom má tento právny zástupca sídlo alebo pobyt. Informácie o právnom zástupcovi sa sprístupnia verejnosti.

ODDIEL VI
ZÁVEREČNÉ USTANOVENIA

Článok 17

Určenie príslušných orgánov

1. Každý členský štát určí orgán alebo orgány príslušné na:

   (a) vydanie príkazov na odstránenie podľa článku 4;

   (b) zistenie, identifikovanie a hlásenie teroristického obsahu poskytovateľom hostingových služieb podľa článku 5;

   (c) dohľad nad vykonávaním proaktívnych opatrení podľa článku 6;

   (d) presadzovanie povinností vyplývajúcich z tohto nariadenia prostredníctvom sankcií podľa článku 18.

2. Členské štáty oznámia Komisii príslušný ***orgán alebo*** orgány uvedené v odseku 1 najneskôr [***dvanásť*** *[...] mesiacov po nadobudnutí účinnosti tohto nariadenia*]. Komisia uverejní oznámenie a všetky jeho zmeny v *Úradnom vestníku Európskej únie*.

Článok 18

Sankcie

1. Členské štáty stanovia pravidlá týkajúce sa sankcií uplatniteľných pri porušení povinností poskytovateľov hostingových služieb podľa tohto nariadenia a prijmú všetky nevyhnutné opatrenia na zabezpečenie ich vykonávania. Takéto sankcie sa obmedzia na porušenie povinností podľa:

   (a) článku 3 ods. 2 (podmienky poskytovateľov hostingových služieb);

   (b) článku 4 ods. 2 a 6 (vykonávanie príkazov na odstránenie a spätná väzba k nim);

(c) článku 5 ods. 5 a 6 (hodnotenie hlásení a spätná väzba k nim);

(d) článku 6 ods. 2 a 4 (správy o proaktívnych opatreniach a prijatie opatrení na základe rozhodnutia, ktorým sa ukladajú osobitné proaktívne opatrenia);

(e) článku 7 (uchovávanie údajov);

(f) článku 8 (transparentnosť);

(g) článku 9 (záruky v súvislosti s proaktívnymi opatreniami);

(h) článku 10 (postupy podávania sťažností);

(i) článku 11 (informácie pre poskytovateľov obsahu);

(j) článku 13 ods. 4 (informácie o dôkazoch o teroristických trestných činoch);

(k) článku 14 ods. 1 (kontaktné miesta);

(l) článku 16 (určenie právneho zástupcu).

2. Ustanovené sankcie musia byť účinné, primerané a odrádzajúce. Členské štáty najneskôr do [*mesiacov od nadobudnutia účinnosti tohto nariadenia*] oznámia tieto pravidlá a opatrenia Komisii a bezodkladne jej oznámia všetky následné zmeny, ktoré sa ich týkajú.

3. Členské štáty zabezpečia, aby príslušné orgány pri určovaní druhu a úrovne sankcií zohľadnili všetky relevantné okolnosti vrátane:

(a) povahy, závažnosti a dĺžky trvania porušenia;

(b) úmyselného alebo nedbanlivostného charakteru porušenia;

(c) predchádzajúcich porušení, ktorých sa dopustila zodpovedná právnická ***alebo fyzická*** osoba;

(d) finančnej sily zodpovednej právnickej ***alebo fyzickej*** osoby;

(e) úrovne spolupráce poskytovateľa hostingových služieb s príslušnými orgánmi.

4. Členské štáty zabezpečia, aby systematické neplnenie si povinností podľa článku 4 ods. 2 podliehalo finančným sankciám až do výšky 4 % celosvetového obratu poskytovateľa hostingových služieb za posledné účtovné obdobie.

Článok 19

Technické požiadavky a zmeny vzorov príkazov na odstránenie

1. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 20 s cieľom doplniť toto nariadenie o technické požiadavky na elektronické prostriedky, ktoré majú príslušné orgány používať na prenos príkazov na odstránenie.

2. Komisia je splnomocnená prijímať takéto delegované akty s cieľom zmeniť prílohy I, II a III s cieľom účinne riešiť prípadnú potrebu zlepšenia v súvislosti s obsahom formulárov príkazov na odstránenie a formulárov, ktoré sa majú použiť na poskytnutie informácií o nemožnosti vykonať príkaz na odstránenie.

Článok 20

Vykonávanie delegovania právomoci

1. Komisii sa udeľuje právomoc prijímať delegované akty za podmienok stanovených v tomto článku.

2. Právomoc prijímať delegované akty uvedené v článku 19 sa Komisii udeľuje na neurčitý čas odo [*dňa uplatňovania tohto nariadenia*].

3. Delegovanie právomoci uvedené v článku 19 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v Úradnom vestníku Európskej únie alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.

4. Pred prijatím delegovaného aktu Komisia konzultuje s expertmi určenými každým členským štátom v súlade so zásadami stanovenými v Medziinštitucionálnej dohode o lepšej tvorbe práva z 13. apríla 2016.

5. Komisia oznamuje delegovaný akt Európskemu parlamentu a Rade súčasne, a to hneď po jeho prijatí.

6. Delegovaný právny akt prijatý podľa článku 19 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.

Článok 21

Monitorovanie

1. Členské štáty zhromažďujú od svojich príslušných orgánov a poskytovateľov hostingových služieb, ktorí patria pod ich právomoc, informácie o opatreniach, ktoré prijali v súlade s týmto nariadením, a každý rok ich do [31. marca] zašlú Komisii. Tieto informácie zahŕňajú:

   (a) informácie o počte vydaných príkazov na odstránenie a hlásení, počte teroristického obsahu, ktorý bol odstránený, resp. ku ktorému bol znemožnený prístup, ako aj o príslušných časových rámcoch v zmysle článkov 4 a 5;

(b) informácie o konkrétnych proaktívnych opatreniach prijatých podľa článku 6 vrátane množstva teroristického obsahu, ktorý bol odstránený, resp. ku ktorému bol znemožnený prístup, a o príslušných časových rámcoch;

(c) informácie o počte začatých konaní vo veci sťažnosti a o opatreniach prijatých poskytovateľmi hostingových služieb podľa článku 10;

(d) informácie o počte začatých konaní o súdnu nápravu a rozhodnutiach, ktoré prijal príslušný orgán v súlade s vnútroštátnym právom.

2. Najneskôr do [*jedného roka odo dňa začatia uplatňovania tohto nariadenia*] Komisia stanoví podrobný program na monitorovanie výstupov, výsledkov a vplyvov tohto nariadenia. V tomto programe monitorovania sa stanovia ukazovatele a spôsob zhromažďovania údajov a ďalších potrebných dôkazov, ako aj interval ich zhromažďovania. Uvedú sa v ňom opatrenia, ktoré majú Komisia a členské štáty prijať pri zhromažďovaní a analýze údajov a iných dôkazov na monitorovanie pokroku a hodnotenie tohto nariadenia podľa článku 23.

Článok 22

Správa o vykonávaní

Do ... [*dvoch rokov od nadobudnutia účinnosti tohto nariadenia*] predloží Komisia Európskemu parlamentu a Rade správu o uplatňovaní tohto nariadenia. V tejto správe Komisie sa zohľadnia informácie o monitorovaní podľa článku 21 a informácie vyplývajúce z povinností transparentnosti podľa článku 8. Členské štáty poskytnú Komisii informácie potrebné na vypracovanie tejto správy.

Článok 23

Hodnotenie

Najskôr [*tri roky odo dňa začatia uplatňovania tohto nariadenia*] Komisia vykoná hodnotenie tohto nariadenia a predloží Európskemu parlamentu a Rade správu o uplatňovaní tohto nariadenia, ako aj o účinnom fungovaní záruk. Túto správu budú v prípade potreby sprevádzať legislatívne návrhy. Členské štáty poskytnú Komisii informácie potrebné na vypracovanie tejto správy.

Článok 24

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Uplatňuje sa od [po uplynutí ***12*** […] mesiacov od nadobudnutia účinnosti].

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli

Za Európsky parlament *predseda*	*Za Radu* *predseda*