Rada
Európskej únie

V Bruseli 14. septembra 2018
(OR. en)

12129/18

Medziinštitucionálny spis:
2018/0331 (COD)

CT 144
ENFOPOL 450
COTER 114
JAI 881
CYBER 193
TELECOM 288
FREMP 142
AUDIO 64
DROIPEN 127
COHOM 107
CODEC 1468

NÁVRH

Od:	Jordi AYET PUIGARNAU, riaditeľ, v zastúpení generálneho tajomníka Európskej komisie
Dátum doručenia:	12. septembra 2018
Komu:	Jeppe TRANHOLM-MIKKELSEN, generálny tajomník Rady Európskej únie
Č. dok. Kom.:	COM(2018) 640 final
Predmet:	Návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY o predchádzaní šíreniu teroristického obsahu online *Príspevok Európskej komisie k stretnutiu čelných predstaviteľov v Salzburgu, 19. až 20. septembra 2018*

Delegáciám v prílohe zasielame dokument COM(2018) 640 final.

Príloha: COM(2018) 640 final

EURÓPSKA
KOMISIA

V Bruseli 12. 9. 2018
COM(2018) 640 final

2018/0331 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o predchádzaní šíreniu teroristického obsahu online

Príspevok Európskej komisie k stretnutiu čelných predstaviteľov v Salzburgu, 19. až 20. septembra 2018

{SEC(2018) 397 final} - {SWD(2018) 408 final} - {SWD(2018) 409 final}

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

1.1 Dôvody a ciele návrhu

Všadeprítomnosť internetu umožňuje jeho užívateľom komunikovať, pracovať, socializovať sa, tvoriť, získavať a zdieľať informácie a obsah spolu so stovkami miliónov jednotlivcov na celom svete. Internetové platformy znamenajú významný prínos pre hospodársky a sociálny blahobyt používateľov v celej Únii aj mimo nej. Schopnosť osloviť takéto široké publikum s minimálnymi nákladmi však priťahuje aj páchateľov trestnej činnosti, ktorí chcú internet zneužiť na nezákonné účely. Nedávne teroristické útoky v EÚ ukázali, ako teroristi zneužívajú internet na prípravu a nábor priaznivcov, na plánovanie a napomáhanie teroristickej činnosti, na glorifikáciu svojich násilných činov a na vyzývanie ostatných, aby sa pridali a rozsievali strach u širokej verejnosti.

Teroristický obsah zdieľaný online na takéto účely sa šíri prostredníctvom poskytovateľov hostingových služieb, ktorí umožňujú nahrávanie obsahu tretím stranám. Teroristický obsah na internete sa ukázal ako fundamentálny nástroj na radikalizáciu a inšpirovanie útokov tzv. „osamelých vlkov“ pri niekoľkých nedávnych teroristických útokoch v Európe. Takýto obsah má nielen výrazne negatívny vplyv na jednotlivcov a spoločnosť ako celok, ale takisto znižuje aj dôveru používateľov v internet a ovplyvňuje obchodné modely a dobré meno dotknutých spoločností. Teroristi nezneužívajú len veľké platformy sociálnych médií, ale čoraz častejšie aj menších poskytovateľov, ktorí ponúkajú rôzne druhy hostingových služieb po celom svete. Toto zneužívanie internetu zdôrazňuje osobitnú spoločenskú zodpovednosť internetových platforiem za ochranu ich užívateľov pred vystavením teroristickému obsahu, ako aj za vážne bezpečnostné riziká, ktoré tento obsah predstavuje pre celú spoločnosť.

Poskytovatelia hostingových služieb v reakcii na výzvy verejných orgánov zaviedli určité opatrenia na boj proti šíreniu teroristického obsahu prostredníctvom ich služieb. Pokrok sa dosiahol prostredníctvom dobrovoľných rámcov a partnerstiev vrátane internetového fóra EÚ, ktoré bolo spustené v decembri 2015 v rámci Európskeho programu v oblasti bezpečnosti. Internetové fórum EÚ podporuje dobrovoľnú spoluprácu a akcie členských štátov a poskytovateľov hostingových služieb zamerané na zníženie prístupu k teroristickému obsahu na internete a na posilnenie postavenia občianskej spoločnosti s cieľom zvýšiť objem účinnej a alternatívnej argumentácie na internete. Toto úsilie prispelo k intenzívnejšej spolupráci, zlepšeniu reakcií spoločností na hlásenia vnútroštátnych orgánov aj jednotky Europolu pre nahlasovanie internetového obsahu, k zavedeniu dobrovoľných proaktívnych opatrení na zlepšenie automatického odhaľovania teroristického obsahu, zvýšenej spolupráci s daným priemyselným odvetvím – vrátane vytvorenia „databázy hashov“ s cieľom zabrániť tomu, aby sa známy teroristický obsah nahrával na prepojených platformách, ako aj ku zvýšenej transparentnosti celého tohto úsilia. Zatiaľ čo spolupráca v rámci internetového fóra EÚ by mala pokračovať aj v budúcnosti, dobrovoľné dohody preukázali takisto aj svoje limity. Po prvé, nie všetci dotknutí poskytovatelia hostingových služieb sa zapojili do fóra, a po druhé, rozsah a tempo pokroku medzi poskytovateľmi hostingových služieb ako celku nepostačuje na primerané riešenie tohto problému.

Vzhľadom na tieto obmedzenia existuje jasná potreba posilniť opatrenia Európskej únie na boj proti teroristickému obsahu na internete. Komisia 1. marca 2018 prijala odporúčanie o opatreniach na účinné riešenie nezákonného obsahu na internete, pričom vychádzala

z oznámenia Komisie zo septembra 2017[1], ako aj z práce internetového fóra EÚ. Odporúčanie obsahovalo osobitnú kapitolu, v ktorej boli identifikované viaceré opatrenia na účinné hatenie šírenia a zdieľania teroristickej propagandy online, ako napríklad zlepšenie postupu v súvislosti s hláseniami, jednohodinový časový rámec na reakciu na tieto hlásenia, proaktívnejšie odhaľovanie, účinné odstraňovanie a dostatočné záruky na presné posúdenie teroristického obsahu[2].

Potreba posilniť činnosť v súvislosti s teroristickým obsahom online sa premietla aj do výziev členských štátov EÚ, pričom niektoré z nich už prijali právne predpisy alebo ich navrhli. V nadväznosti na sériu teroristických útokov v EÚ a so zreteľom na skutočnosť, že teroristický obsah je naďalej ľahko dostupný online, Európska rada na svojom zasadnutí v dňoch 22. a 23. júna 2017 vyzvala dané odvetvie, aby vyvinulo „nové technológie a nástroje, ktoré zlepšia automatické odhaľovanie obsahu, ktorý podnecuje na páchanie teroristických činov, a jeho odstraňovanie. Dopĺňať by to v prípade potreby mali príslušné legislatívne opatrenia na úrovni EÚ.“ Európska rada na svojom zasadnutí 28. júna 2018 privítala „úmysel Komisie predložiť legislatívny návrh na zlepšenie odhaľovania a odstraňovania obsahu, ktorý podnecuje k nenávisti a páchaniu teroristických činov“. Okrem toho Európsky parlament vo svojom uznesení o online platformách a jednotnom digitálnom trhu 15. júna 2017 vyzval dotknuté platformy, aby „posilnili opatrenia na boj proti nezákonnému a škodlivému obsahu“, a vyzval Komisiu, aby predložila návrhy na riešenie týchto otázok.

V záujme riešenia týchto otázok a v reakcii na výzvy členských štátov a Európskeho parlamentu sa tento návrh Komisie usiluje vytvoriť jasný a harmonizovaný právny rámec, ktorý by zabránil zneužívaniu hostingových služieb na šírenie teroristického obsahu online, a to s cieľom zaručiť hladké fungovanie digitálneho jednotného trhu pri súčasnom zabezpečení dôvery a bezpečnosti. Cieľom tohto nariadenia je vniesť jasno do otázky zodpovednosti poskytovateľov hostingových služieb, pokiaľ ide o prijímanie všetkých vhodných, zmysluplných a primeraných opatrení, ktoré sú potrebné na zaistenie bezpečnosti ich služieb a rýchle a účinné odhaľovanie a odstraňovanie teroristického obsahu online, a to pri zohľadnení zásadného významu slobody prejavu a práva na informácie v otvorenej a demokratickej spoločnosti. V nariadení sa zavádza aj niekoľko potrebných záruk určených na zabezpečenie úplného dodržiavania základných práv, ako je sloboda prejavu a právo na informácie v demokratickej spoločnosti, okrem možností súdnej nápravy zaručených právom na účinný prostriedok nápravy, ktoré sú zakotvené v článku 19 ZEÚ a v článku 47 Charty základných práv EÚ.

Stanovením minimálnej povinnej starostlivosti zo strany poskytovateľov hostingových služieb, ktorá zahŕňa niektoré osobitné pravidlá a povinnosti, ako aj povinností členských štátov, sa v návrhu sleduje cieľ, ktorým je zvýšenie účinnosti súčasných opatrení na odhaľovanie, identifikáciu a odstraňovanie teroristického obsahu online, a to bez zásahu do základných práv, ako je napr. sloboda prejavu a právo na informácie. Takýto harmonizovaný právny rámec uľahčí poskytovanie online služieb na celom jednotnom digitálnom trhu, zabezpečí rovnaké podmienky pre všetkých poskytovateľov hostingových služieb, ktorí smerujú svoje služby do Európskej únie, a poskytne pevný právny rámec na odhaľovanie a odstraňovanie teroristického obsahu spolu s primeranými zárukami na ochranu základných práv. Povinnosťami v oblasti transparentnosti sa predovšetkým zvýši dôvera občanov,

[1] Oznámenie [COM (2017) 555 final] o boji proti nezákonnému obsahu na internete.

[2] Odporúčanie [C (2018) 1177 final] z 1. marca 2018 o opatreniach na účinný boj proti nezákonnému obsahu na internete.

a najmä používateľov internetu, a zlepší sa zodpovednosť a transparentnosť činností spoločností, a to aj pokiaľ ide o verejné orgány. V návrhu nariadenia sa takisto stanovuje povinnosť zaviesť prostriedky nápravy a mechanizmy na podávanie sťažností, aby sa zabezpečilo, že používatelia môžu napadnúť odstránenie svojho obsahu. Povinnosti ukladané členským štátom prispejú k týmto cieľom, ako aj k zlepšeniu schopnosti príslušných orgánov prijímať primerané opatrenia proti teroristickému obsahu online a bojovať proti trestnej činnosti. Ak poskytovatelia hostingových služieb nebudú dodržiavať nariadenie, členské štáty budú môcť uložiť sankcie.

1.2 Súlad s existujúcim právnym rámcom EÚ v tejto oblasti politiky

Tento návrh je v súlade s *acquis*, ktoré sa vzťahuje na jednotný digitálny trh, a najmä so smernicou o elektronickom obchode. Predovšetkým by žiadne opatrenia, ktoré prijal poskytovateľ hostingových služieb v súlade s týmto nariadením, vrátane akýchkoľvek proaktívnych opatrení, nemali samé o sebe viesť k tomu, že tento poskytovateľ služieb príde o výhodu výnimky zo zodpovednosti, ktorá za určitých podmienok stanovuje v článku 14 smernice o elektronickom obchode. Rozhodnutie vnútroštátnych orgánov uložiť primerané a osobitné proaktívne opatrenia by v zásade nemalo viesť k uloženiu všeobecnej povinnosti monitorovať, ako sa vymedzuje v článku 15 ods. 1 smernice 2000/31/ES, členským štátom. Vzhľadom na mimoriadne závažné riziká spojené so šírením teroristického obsahu by sa však rozhodnutia podľa tohto nariadenia mali mať možnosť výnimočne odchýliť od tejto zásady podľa rámca EÚ. Pred prijatím takýchto rozhodnutí by príslušný orgán mal dosiahnuť spravodlivú rovnováhu medzi potrebou verejnej bezpečnosti a dotknutými záujmami a príslušnými základnými právami, najmä právom na slobodu prejavu a právom na informácie, ako aj slobodou podnikania a ochranou osobných údajov a súkromia. Povinná starostlivosť uložená poskytovateľom hostingových služieb by mala odzrkadľovať a rešpektovať túto rovnováhu, ktorá je vyjadrená v smernici o elektronickom obchode.

Návrh je takisto v súlade a úzko prepojený so smernicou (EÚ) 2017/541 o boji proti terorizmu, ktorej cieľom je harmonizovať právne predpisy členských štátov, ktorými sa stanovuje trestnosť teroristických trestných činov. V článku 21 smernice o boji proti terorizmu sa vyžaduje, aby členské štáty prijali opatrenia na zabezpečenie rýchleho odstránenia online obsahu, ktorý predstavuje verejné podnecovanie na spáchanie trestného činu terorizmu, pričom výber opatrení sa v ňom ponecháva na členských štátoch. Toto nariadenie sa so zreteľom na svoju preventívnu povahu vzťahuje nielen na materiál podnecujúci na terorizmus, ale aj na materiál na účely náboru alebo výcviku, v čom sa odzrkadľujú iné trestné činy súvisiace s teroristickými činnosťami, na ktoré sa takisto vzťahuje smernica (EÚ) 2017/541. Týmto nariadením sa priamo ukladá povinná starostlivosť poskytovateľom hostingových služieb, v rámci ktorej sú povinní odstrániť teroristický obsah, a harmonizujú postupy týkajúce sa príkazov na odstránenie s cieľom obmedziť prístup k teroristickému obsahu online.

Nariadením sa dopĺňajú pravidlá stanovené v pripravovanej smernici o audiovizuálnych mediálnych službách, keďže osobný a vecný rozsah pôsobnosti nariadenia je širší. Nariadenie sa nevzťahuje len na platformy na zdieľanie videí, ale na všetky druhy poskytovateľov hostingových služieb. Okrem toho sa vzťahuje nielen na videá, ale aj obrázky a text. Toto nariadenie okrem toho presahuje rámec predmetnej smernice, pokiaľ ide o hmotnoprávne ustanovenia, a to harmonizáciou pravidiel týkajúcich sa žiadostí o odstránenie teroristického obsahu, ako aj proaktívnych opatrení.

Navrhované nariadenie vychádza z odporúčania Komisie o nezákonnom obsahu[3] z marca 2018. Odporúčanie zostáva platným, a všetci, ktorí zohrávajú úlohu pri znižovaní prístupu k nezákonnému obsahu vrátane teroristického obsahu, by mali pokračovať v zosúlaďovaní svojich snáh s opatreniami identifikovanými v rámci tohto odporúčania.

1.3 Zhrnutie návrhu nariadenia

Osobná pôsobnosť návrhu zahŕňa poskytovateľov hostingových služieb, ktorí ponúkajú svoje služby v rámci Únie, bez ohľadu na miesto ich usadenia alebo ich veľkosť. V navrhovanom predpise sa zavádza niekoľko opatrení na predchádzanie zneužívaniu hostingových služieb na šírenie teroristického obsahu online s cieľom zaručiť hladké fungovanie jednotného digitálneho trhu pri súčasnom zabezpečení dôvery a bezpečnosti. Vymedzenie pojmu nezákonný teroristický obsah je v súlade s vymedzením teroristických trestných činov obsiahnutým v smernici (EÚ) 2017/541, pričom tento pojem sa vymedzuje ako informácie, ktoré sa používajú na podnecovanie na spáchanie teroristických trestných činov a glorifikáciu ich spáchania, na podporovanie účasti na páchaní takýchto trestných činov a na poskytnutie pokynov na ich páchanie, ako aj na podporu účasti v teroristických skupinách.

V záujme zabezpečenia odstránenia nezákonného teroristického obsahu sa v nariadení zavádza príkaz na odstránenie, ktorý môže byť vydaný vo forme administratívneho alebo súdneho rozhodnutia príslušného orgánu členského štátu. V takýchto prípadoch je poskytovateľ hostingových služieb povinný odstrániť obsah, resp. znemožniť k nemu prístup, do jednej hodiny. Nariadením sa okrem toho harmonizujú minimálne požiadavky na hlásenia zasielané príslušnými orgánmi členských štátov a orgánmi Únie (napr. Europol) poskytovateľom hostingových služieb, ktorí ich posudzujú na základe vlastných podmienok. V nariadení sa napokon vyžaduje, aby poskytovatelia hostingových služieb prijímali v prípade potreby proaktívne opatrenia primerané úrovni rizika a odstránili teroristický materiál zo svojich služieb, a to aj zavedením automatizovaných nástrojov odhaľovania.

Opatrenia, ktorých cieľom je obmedziť teroristický obsah online, sú sprevádzané niekoľkými kľúčovými zárukami na zabezpečenie úplnej ochrany základných práv. V návrhu sa ako súčasť opatrení na ochranu pred chybným odstránením obsahu, ktorý nie je teroristický, stanovuje povinnosť zaviesť opatrenia na nápravu a mechanizmy na podávanie sťažností, aby sa zabezpečilo, že používatelia budú môcť napadnúť odstránenie svojho obsahu. V nariadení sa okrem toho zavádzajú povinnosti týkajúce sa transparentnosti, pokiaľ ide o opatrenia proti teroristickému obsahu zo strany poskytovateľov hostingových služieb, čím sa zabezpečuje zodpovednosť voči používateľom, občanom a orgánom verejnej moci.

Nariadenie ukladá členským štátom aj povinnosť zabezpečiť, aby ich príslušné orgány mali kapacity potrebné na to, aby boli schopné zasiahnuť proti teroristickému obsahu na internete. Okrem toho sú členské štáty povinné navzájom informovať sa a spolupracovať, pričom môžu využívať kanály zriadené Europolom na zabezpečenie koordinácie, pokiaľ ide o príkazy na odstránenie a hlásenia. V nariadení sa stanovuje aj povinnosť poskytovateľov hostingových služieb podrobnejšie informovať o prijatých opatreniach a takisto aj povinnosť poskytnúť orgánom presadzovania práva informácie v prípade, že odhalia obsah, ktorý predstavuje hrozbu pre život alebo bezpečnosť. Napokon sa v nariadení navrhuje povinnosť poskytovateľov hostingových služieb uchovať obsah, ktorý odstraňujú, čo má fungovať ako záruka proti chybnému odstráneniu a zabezpečiť, aby nedošlo k strate potenciálnych dôkazov

[3] Odporúčanie [C (2018) 1177 final] z 1. marca 2018 o opatreniach na účinný boj proti nezákonnému obsahu na internete.

na účely predchádzania teroristickým trestným činom a ich odhaľovania, vyšetrovania a stíhania.

2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

2.1 Právny základ

Právnym základom je článok 114 Zmluvy o fungovaní Európskej únie, v ktorom sa stanovujú opatrenia na zabezpečenie fungovania vnútorného trhu.

Článok 114 predstavuje vhodný právny základ na zosúladenie podmienok pre poskytovateľov hostingových služieb pri poskytovaní cezhraničných služieb na jednotnom digitálnom trhu a na riešenie rozdielov medzi ustanoveniami členských štátov, ktoré by inak mohli brániť fungovaniu vnútorného trhu. Takisto zabraňuje vzniku budúcich prekážok hospodárskej činnosti, ktoré by mohli vzniknúť v dôsledku rozdielneho vývoja vnútroštátnych právnych predpisov.

Článok 114 ZFEÚ sa môže použiť aj na uloženie povinností poskytovateľom služieb usadeným mimo územia EÚ, ak poskytovanie ich služieb má vplyv na vnútorný trh, keďže je to potrebné na dosiahnutie požadovaného cieľa vnútorného trhu.

2.2 Výber nástroja

V článku 114 ZFEÚ sa zákonodarcom v Únii poskytuje možnosť prijímať nariadenia a smernice.

Keďže návrh sa týka povinností poskytovateľov služieb, ktorí zvyčajne ponúkajú svoje služby vo viac ako jednom členskom štáte, rozdielnosť v uplatňovaní týchto pravidiel by bránila poskytovaniu služieb poskytovateľmi pôsobiacimi vo viacerých členských štátoch. Nariadenie umožňuje, aby sa tá istá povinnosť uložila jednotným spôsobom v celej Únii, pričom je priamo uplatniteľné, prináša zrozumiteľnosť a väčšiu právnu istotu a zabraňuje odlišnej transpozícii v členských štátoch. Z týchto dôvodov sa za najvhodnejšiu formu pre tento nástroj považuje nariadenie.

2.3 Subsidiarita

Vzhľadom na cezhraničný rozmer riešených problémov si dosiahnutie cieľov vyžaduje, aby sa opatrenia, ktoré sú súčasťou návrhu, prijali na úrovni Únie. Internet má už zo svojej podstaty cezhraničný charakter a obsah, ktorý sa nachádza v jednom členskom štáte, je zvyčajne dostupný z akéhokoľvek iného členského štátu.

Dochádza k roztrieštenosti rámca rôznych vnútroštátnych pravidiel na boj proti teroristickému obsahu na internete a riziká sa zvyšujú. To by viedlo k záťaži pre spoločnosti v súvislosti s dodržiavaním rozdielnych právnych predpisov a k vytvoreniu nerovnakých podmienok pre spoločnosti, ako aj k vzniku bezpečnostných nedostatkov.

Opatrenia na úrovni EÚ preto zvyšujú právnu istotu a účinnosť opatrení poskytovateľov hostingových služieb na boj proti teroristickému obsahu online. Tým by sa malo umožniť viacerým spoločnostiam, aby prijali opatrenia, a to aj pokiaľ ide o spoločnosti usadené mimo Európskej únie, čím sa posilní integrita jednotného digitálneho trhu.

Toto sú dôvody, pre ktoré je nutné konať na úrovni EÚ, ktoré boli vyjadrené aj v záveroch Európskej rady z júna 2018, v ktorých sa Komisia vyzýva, aby v tejto oblasti predložila legislatívny návrh.

2.4 Proporcionalita

V návrhu sa stanovujú pravidlá pre poskytovateľov hostingových služieb, aby uplatňovali opatrenia na urýchlené odstránenie teroristického obsahu zo svojich služieb. Hlavné prvky návrhu ho obmedzujú len na to, čo je nevyhnutné na dosiahnutie cieľov realizovaných politík.

V návrhu sa zohľadňuje záťaž poskytovateľov hostingových služieb a záruky vrátane ochrany slobody prejavu a práva na informácie, ako aj iných základných práv. Jednohodinový rámec na odstránenie sa vzťahuje len na príkazy na odstránenie, v prípade ktorých príslušné orgány konštatovali nezákonnosť v súdne preskúmateľnom rozhodnutí. Pokiaľ ide o hlásenia, existuje povinnosť zaviesť opatrenia na uľahčenie rýchleho posúdenia teroristického obsahu, avšak bez toho, aby bola uložená aj povinnosť odstrániť ho, a neexistuje ani povinnosť urobiť tak v rámci absolútnych lehôt. Konečné rozhodnutie zostáva aj naďalej dobrovoľným rozhodnutím poskytovateľa hostingových služieb. Záťaž spoločností spojená s hodnotením obsahu sa zmierňuje tým, že príslušné orgány členských štátov a subjekty Únie poskytujú vysvetlenia, prečo sa obsah môže považovať za teroristický. Poskytovatelia hostingových služieb v prípade potreby prijmú proaktívne opatrenia na ochranu svojich služieb pred šírením teroristického obsahu. Osobitné povinnosti týkajúce sa proaktívnych opatrení sa vzťahujú len na tých poskytovateľov hostingových služieb, ktorí sú vystavení teroristickému obsahu, čo dokazuje skutočnosť, že boli adresátmi príkazu na odstránenie, ktorý sa stal konečným, pričom tieto osobitné povinnosti by mali byť úmerné úrovni rizika, ako aj zdrojom spoločnosti. Uchovávanie odstráneného obsahu a súvisiacich údajov sa obmedzuje na časové obdobie primerané účelu konania v rámci správneho alebo súdneho preskúmania a účelu predchádzania teroristickým trestným činom a ich odhaľovania, vyšetrovania a stíhania.

3. VÝSLEDKY HODNOTENÍ EX POST, KONZULTÁCIÍ SO ZAINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

3.1 Konzultácie so zainteresovanými stranami

Pri príprave tohto legislatívneho návrhu Komisia konzultovala so všetkými príslušnými zainteresovanými stranami s cieľom pochopiť ich názory a prípadné možnosti napredovania. Komisia uskutočnila otvorenú verejnú konzultáciu o opatreniach na zlepšenie účinnosti boja proti nezákonnému obsahu, pričom dostala 8961 odpovedí, z ktorých 8749 bolo od jednotlivcov, 172 od organizácií, 10 od orgánov verejnej správy a 30 od ostatných kategórií respondentov. Súbežne sa uskutočnil prieskum Eurobarometra s náhodnou vzorkou 33 500 obyvateľov EÚ, ktorý bol zameraný na problematiku nezákonného obsahu online. Komisia počas mája a júna 2018 konzultovala s orgánmi členských štátov aj s poskytovateľmi hostingových služieb, pokiaľ ide o konkrétne opatrenia na boj proti teroristickému obsahu online.

Väčšina zainteresovaných strán vyjadrila názor, že teroristický obsah online je vážnym spoločenským problémom, ktorý má vplyv na používateľov internetu a obchodné modely poskytovateľov hostingových služieb. Vo všeobecnejšej rovine, 65 % respondentov prieskumu Eurobarometra[4] uviedlo názor, že internet nie je pre používateľov bezpečný, a 90 % respondentov považuje za dôležité, aby sa obmedzilo šírenie nezákonného obsahu online. Z konzultácií s členskými štátmi vyplynulo, že aj keď dobrovoľné dohody prinášajú výsledky, mnohé z členských štátov sa domnievajú, že sú potrebné záväzné povinnosti týkajúce sa teroristického obsahu, čo bol aj postoj, ktorý sa odrazil v záveroch Európskej rady z júna 2018. Hoci sa poskytovatelia hostingových služieb celkovo vyslovili za pokračovanie

[4] Eurobarometer 469 o nezákonnom obsahu na internete, jún 2018.

dobrovoľných opatrení, poukázali na potenciálne negatívne účinky vznikajúcej právnej fragmentácie v Únii.

Mnohé zainteresované strany sa takisto vyjadrili, že je potrebné zabezpečiť, aby všetky regulačné opatrenia na odstránenie obsahu, najmä proaktívne opatrenia a prísne časové rámce, boli vyvážené zárukami v oblasti základných práv, najmä slobody prejavu. Zainteresované strany pomenovali množstvo potrebných opatrení týkajúcich sa transparentnosti, zodpovednosti, ako aj ľuďmi vykonávaného preskúmania v prípade využívania automatizovaných nástrojov.

3.2 Posúdenia vplyvu

Výbor pre kontrolu regulácie vydal kladné stanovisko k posúdeniu vplyvu spolu s výhradami a predložil rôzne návrhy na zlepšenie[5]. V nadväznosti na toto stanovisko bola správa o posúdení vplyvu zmenená s cieľom riešiť hlavné pripomienky tohto výboru, pričom sa dôraz kládol najmä na teroristický obsah, a to pri súčasnom zdôraznení dôsledkov na fungovanie jednotného digitálneho trhu, ako aj na podrobnejšiu analýzu vplyvu na základné práva a fungovanie záruk navrhnutých v rámci jednotlivých posudzovaných možností.

Ak sa neprijmú žiadne dodatočné opatrenia, očakáva sa, že dobrovoľné opatrenia v rámci základného scenára budú pokračovať a budú mať určitý vplyv na znižovanie teroristického obsahu online. Je však nepravdepodobné, že by dobrovoľné opatrenia prijali všetci poskytovatelia hostingových služieb vystavení takémuto obsahu, pričom možno očakávať ďalšiu právnu fragmentáciu, ktorá prinesie dodatočné prekážky pre cezhraničné poskytovanie služieb. Okrem základného scenára sa zvažovali tri hlavné možnosti politiky s rastúcou úrovňou účinnosti, pokiaľ ide o plnenie cieľov stanovených v posúdení vplyvu a celkového politického cieľa, ktorým je zníženie teroristického obsahu na internete.

Rozsah týchto povinností bol pri všetkých troch posudzovaných možnostiach politík zameraný na všetkých poskytovateľov hostingových služieb (osobná pôsobnosť) usadených v EÚ, ako aj v tretích krajinách, ak títo poskytovatelia ponúkajú svoje služby v Únii (územná pôsobnosť). So zreteľom na povahu problému a potrebu zabrániť zneužívaniu menších platforiem sa pre MSP v rámci žiadnej zo zvažovaných možností nepredpokladajú žiadne výnimky. V rámci všetkých zvažovaných možností by sa zaviedla povinnosť pre poskytovateľov hostingových služieb, aby určili právneho zástupcu v EÚ – a to aj pokiaľ ide o spoločnosti usadené mimo EÚ – s cieľom zabezpečiť vykonateľnosť pravidiel EÚ. Takisto sa v rámci všetkých možností predpokladalo, že členské štáty zavedú sankčné mechanizmy.

Pri všetkých možnostiach sa takisto rátalo s vytvorením nového harmonizovaného systému na práve založených príkazov na odstránenie teroristického obsahu online, ktoré by vydávali vnútroštátne orgány a ktoré by boli určené poskytovateľom hostingových služieb, ako aj s požiadavkou odstrániť tento obsah do jednej hodiny. Tieto príkazy si nemusia nevyhnutne vyžadovať posúdenie zo strany poskytovateľov hostingových služieb a budú podliehať súdnemu preskúmaniu.

Spoločnými prvkami všetkých troch posudzovaných možností boli záruky, a to najmä postupy podávania sťažností a účinné prostriedky nápravy vrátane súdnej nápravy, ako aj iné ustanovenia na predchádzanie chybnému odstraňovaniu obsahu, ktorý nie je teroristický, a zároveň zabezpečenie dodržiavania základných práv. Okrem toho všetky možnosti zahŕňajú povinnosti týkajúce sa podávania správ ako formy verejnej transparentnosti, ako aj podávanie

[5] Odkaz na stanovisko výboru pre kontrolu regulácie v RegDoc.

správ členským štátom a Komisii aj príslušným orgánom v prípade, že existuje podozrenie z páchania trestnej činnosti. Ďalej sa predpokladali povinnosti týkajúce sa spolupráce medzi vnútroštátnymi orgánmi, poskytovateľmi hostingových služieb a v príslušných prípadoch aj s Europolom.

Hlavné rozdiely medzi troma možnosťami sa týkali rozsahu vymedzenia pojmu teroristický obsah, miery harmonizácie hlásení, rozsahu proaktívnych opatrení, koordinačných povinností členských štátov, ako aj požiadaviek na uchovávanie údajov. Možnosť č. 1 by na základe úzkeho vymedzenia obmedzila vecnú pôsobnosť na obsah šírený s cieľom priamo navádzať na páchanie teroristického činu, zatiaľ čo možnosti č. 2 a č. 3 by znamenali komplexnejší prístup, ktorý by zahŕňal aj materiál týkajúci sa náboru a výcviku. Pokiaľ ide o proaktívne opatrenia, v rámci možnosti č. 1 by poskytovatelia hostingových služieb vystavení teroristickému obsahu museli vykonať posúdenie rizika, avšak proaktívne opatrenia na riešenie tohto rizika by zostali dobrovoľné. Možnosť č. 2 by vyžadovala od poskytovateľov hostingových služieb, aby pripravili akčný plán, ktorý môže zahŕňať aj zavedenie automatizovaných nástrojov na predchádzanie opakovanému nahrávaniu už odstráneného obsahu. Možnosť č. 3 zahŕňa komplexnejšie proaktívne opatrenia, ktoré od poskytovateľov služieb vystavených teroristickému obsahu vyžadujú, aby identifikovali aj nový materiál. Pri všetkých posudzovaných možnostiach by požiadavky týkajúce sa proaktívnych opatrení boli primerané úrovni vystavenia teroristickému materiálu, ako aj ekonomickým možnostiam poskytovateľa služieb. Pokiaľ ide o hlásenia, pri možnosti č. 1 by nedochádzalo k harmonizácii prístupu k hláseniam, zatiaľ čo pri možnosti č. 2 by sa o harmonizácii uvažovalo len v súvislosti s hláseniami Europolu, a pri možnosti č. 3 by popri jeho hláseniach boli harmonizované aj hlásenia členských štátov. V rámci možností č. 2 a č. 3 by členské štáty boli povinné informovať sa, koordinovať sa a spolupracovať navzájom a pri možnosti č. 3 by mali takisto aj povinnosť zabezpečiť, aby ich príslušné orgány mali kapacity na odhaľovanie a oznamovanie teroristického obsahu. A napokon možnosť č. 3 obsahuje aj požiadavku na uchovanie údajov ako záruku pre prípad chybného odstránenia a na uľahčenie vyšetrovania trestných činov.

Popri právnych ustanoveniach sa uvažovalo, že všetky legislatívne možnosti budú sprevádzané súborom podporných opatrení, najmä s cieľom uľahčiť spoluprácu medzi vnútroštátnymi orgánmi a Europolom, ako aj spoluprácu s poskytovateľmi hostingových služieb, ako aj podporu výskumu, vývoja a inovácií na rozvoj a zavádzanie technologických riešení. Po prijatí právneho nástroja by sa mohli zaviesť aj ďalšie nástroje na zvyšovanie informovanosti a podporné nástroje pre MSP.

V posúdení vplyvu sa dospelo k záveru, že na dosiahnutie cieľa politiky je potrebný rad opatrení. Komplexné vymedzenie pojmu teroristický obsah, ktoré by zahŕňalo najškodlivejší materiál, by bolo vhodnejšie ako úzke vymedzenie obsahu (možnosť č. 1). Proaktívne povinnosti obmedzené na prevenciu opätovného nahrávania teroristického obsahu (možnosť č. 2) by predstavovali menší zásah než povinnosti súvisiace s odhaľovaním nového teroristického obsahu (možnosť č. 3). Ustanovenia o hláseniach by sa mali vzťahovať na hlásenia z Europolu aj z členských štátov (možnosť č. 3), a teda nielen na hlásenia z Europolu (možnosť č. 2), pretože hlásenia z členských štátov sú dôležitým príspevkom v rámci celkového úsilia o znižovanie prístupu k teroristickému obsahu online. Tieto opatrenia by sa mali implementovať spolu s opatreniami, ktoré sú spoločné pre všetky možnosti, vrátane spoľahlivých záruk proti chybnému odstraňovaniu obsahu.

3.3 Základné práva

Teroristická propaganda online sa snaží podnecovať jednotlivcov, aby vykonali teroristické útoky, a to aj tým, že im poskytuje podrobné pokyny o tom, ako spôsobiť maximálnu ujmu. Po spáchaní týchto násilných činov nasleduje ďalšia propaganda, ktorá tieto činy glorifikuje, a zároveň vyzýva ostatných, aby sa pridali. Toto nariadenie prispieva k ochrane verejnej bezpečnosti tým, že znižuje dostupnosť teroristického obsahu, ktorý podporuje porušovanie základných práv a motivuje naň.

Návrh by mohol mať potenciálne vplyv na viacero základných práv:

a) práva poskytovateľa obsahu: právo na slobodu prejavu; právo na ochranu osobných údajov; právo na rešpektovanie súkromného a rodinného života, zásadu nediskriminácie a právo na účinný prostriedok nápravy;

b) práva poskytovateľa služieb: právo na slobodu podnikania; právo na účinný prostriedok nápravy;

c) práva všetkých občanov: a právo na slobodu prejavu a právo na informácie.

Vzhľadom na príslušné *acquis* sú v navrhovanom nariadení zahrnuté primerané a spoľahlivé záruky na zabezpečenie ochrany práv týchto osôb.

Prvým prvkom je v tomto kontexte skutočnosť, že v nariadení sa stanovuje vymedzenie pojmu teroristický obsah online v súlade s vymedzením teroristických trestných činov v smernici (EÚ) 2017/541. Toto vymedzenie pojmu sa vzťahuje na príkazy na odstránenie a hlásenia, ako aj na proaktívne opatrenia. Týmto vymedzením sa zabezpečuje, aby sa odstránil iba nezákonný obsah, ktorý zodpovedá vymedzeniu súvisiacich trestných činov v rámci celej Únie. Návrh nariadenia ďalej zahŕňa aj všeobecnú povinnú starostlivosť poskytovateľov hostingových služieb, ktorí musia 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 teroristický.

Konkrétnejšie, nariadenie bolo navrhnuté s cieľom zabezpečiť proporcionalitu opatrení prijatých v súvislosti so základnými právami. Pokiaľ ide o príkazy na odstránenie, posúdenie obsahu (podľa potreby aj z právneho hľadiska), ktoré vykoná príslušný orgán, odôvodňuje stanovenie lehoty v trvaní jednej hodiny na vykonanie tohto príkazu. Okrem toho ustanovenia v tomto nariadení, ktoré sa týkajú hlásení, platia len pre tie hlásenia, ktoré zaslali príslušné orgány a subjekty Únie a v ktorých sa ozrejmuje, prečo môže byť určitý obsah považovaný za teroristický. Hoci zodpovednosť za odstránenie obsahu identifikovaného v hlásení leží naďalej na poskytovateľovi hostingových služieb, toto jeho rozhodnutie je uľahčené uvedeným posúdením.

V prípade proaktívnych opatrení zodpovednosť za identifikáciu, hodnotenie a odstránenie obsahu nesú aj naďalej poskytovatelia hostingových služieb a vyžaduje sa od nich, aby zaviedli záruky, ktoré zabezpečia, že obsah nebude chybne odstránený, a to aj prostredníctvom ľuďmi vykonávaného preskúmania, a to najmä v prípade potreby ďalšej kontextualizácie. Okrem toho, na rozdiel od základného scenára, v ktorom najviac postihnuté spoločnosti zriaďovali automatizované nástroje bez verejného dohľadu, by návrh opatrení, ako aj ich vykonávanie podliehali oznamovacej povinnosti príslušným orgánom v členských štátoch. Táto povinnosť znižuje riziká chybných odstránení tak pre spoločnosti, ktoré vytvárajú nové nástroje, ako aj pre tých, ktorí ich už používajú. Okrem toho sa od

poskytovateľov hostingových služieb vyžaduje, aby poskytli poskytovateľom obsahu užívateľsky ústretové mechanizmy na podávanie sťažností s cieľom napadnúť rozhodnutie o odstránení ich obsahu, a aby uverejňovali správy na účely transparentnosti pre širokú verejnosť.

Nakoniec, ak by sa mal akýkoľvek obsah a súvisiace údaje odstrániť chybne aj napriek týmto zárukám, poskytovatelia hostingových služieb sú povinní ho uchovávať počas šiestich mesiacov, aby ho mohli obnoviť, čo je v záujme zabezpečenia účinnosti sťažností a postupov preskúmania so zreteľom na ochranu slobody prejavu a informácií. Toto uchovávanie zároveň prispieva aj k presadzovaniu práva. Poskytovatelia hostingových služieb musia zaviesť technické a organizačné záruky na zabezpečenie toho, aby sa údaje nepoužívali na iné účely.

Navrhované opatrenia, najmä tie, ktoré súvisia s príkazmi na odstránenie, hláseniami, proaktívnymi opatreniami a uchovávaním údajov, by nemali len chrániť používateľov internetu pred teroristickým obsahom, ale takisto by mali prispievať k ochrane práva občanov na život znižovaním dostupnosti teroristického obsahu online.

4. VPLYV NA ROZPOČET

Legislatívny návrh nariadenia nemá vplyv na rozpočet Únie.

5. ĎALŠIE PRVKY

5.1 Plány vykonávania, spôsob monitorovania, hodnotenia a podávania správ

Komisia do [jedného roka od dátumu uplatňovania tohto nariadenia] zriadi podrobný program monitorovania 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 zbere a analýze údajov a iných dôkazov na monitorovanie pokroku a hodnotenie tohto nariadenia.

Na základe stanoveného programu monitorovania Komisia do dvoch rokov od nadobudnutia účinnosti tohto nariadenia podá správu o vykonávaní tohto nariadenia na základe správ na účely transparentnosti, ktoré uverejnili spoločnosti, ako aj na základe informácií, ktoré poskytli členské štáty. Komisia vykoná hodnotenie najskôr štyri roky po nadobudnutí účinnosti nariadenia.

Na základe zistení z hodnotenia vrátane toho, či pretrvávajú určité medzery alebo slabé miesta, a so zreteľom na technologický vývoj, Komisia posúdi potrebu rozšírenia rozsahu pôsobnosti nariadenia. Komisia v prípade potreby predloží návrhy na zmenu tohto nariadenia.

Komisia podporí vykonávanie, monitorovanie a hodnotenie nariadenia prostredníctvom expertnej skupiny Komisie. Táto skupina takisto uľahčí spoluprácu medzi poskytovateľmi hostingových služieb, orgánmi presadzovania práva a Europolom, podporí výmeny a postupy na odhaľovanie a odstraňovanie teroristického obsahu, poskytne odborné znalosti o vývoji *modu operandi* teroristov online a v prípade potreby poskytne poradenstvo a usmernenie s cieľom umožniť vykonávanie ustanovení.

Vykonávanie navrhovaného nariadenia by sa mohlo uľahčiť prostredníctvom niekoľkých podporných opatrení. Medzi ne patrí možný vývoj platformy v rámci Europolu s cieľom napomôcť koordináciu hlásení a príkazov na odstránenie. Výskum zameraný na zmeny

v spôsobe fungovania teroristov, ktorý financuje EÚ, zlepšuje porozumenie a informovanosť všetkých príslušných zainteresovaných strán. Okrem toho sa v rámci programu Horizont 2020 podporuje výskum zameraný na vývoj nových technológií vrátane automatizovanej prevencie nahrávania teroristického obsahu. Komisia bude okrem toho naďalej analyzovať, ako podporovať príslušné orgány a poskytovateľov hostingových služieb pri vykonávaní tohto nariadenia prostredníctvom finančných nástrojov EÚ.

5.2 Podrobné vysvetlenie konkrétnych ustanovení návrhu

V článku 1 sa stanovuje predmet úpravy tak, že sa v ňom uvádza, že v nariadení sa stanovujú pravidlá na predchádzanie zneužívaniu hostingových služieb na šírenie teroristického obsahu online vrátane povinnej starostlivosti poskytovateľov hostingových služieb a opatrení, ktoré majú členské štáty zaviesť. Takisto sa v ňom stanovuje územná pôsobnosť, a to tak, že zahŕňa poskytovateľov hostingových služieb, ktorí ponúkajú služby v Únii, bez ohľadu na to, kde sú usadení.

V článku 2 sa stanovuje vymedzenie pojmov používaných v návrhu. Takisto sa v ňom definuje teroristický obsah na preventívne účely, a to na základe smernice o boji proti terorizmu, a to s cieľom zahrnúť materiál a informácie, ktoré nabádajú na páchanie teroristických trestných činov alebo na poskytnutie pomoci pri páchaní týchto činov, resp. na ne motivujú alebo ich ospravedlňujú, ako aj ktoré predstavujú pokyny na páchanie takýchto trestných činov alebo ktoré podporujú účasť na činnostiach teroristickej skupiny.

V článku 3 sa stanovuje povinná starostlivosť, ktorú majú uplatňovať poskytovatelia hostingových služieb pri prijímaní opatrení v súlade s týmto nariadením, a to najmä s náležitým ohľadom na príslušné základné práva. Stanovujú sa v ňom vhodné ustanovenia, ktoré sa majú zaviesť v rámci podmienok poskytovateľov hostingových služieb, ako aj s cieľom zabezpečiť ich následné uplatňovanie.

V článku 4 sa členským štátom ukladá povinnosť splnomocniť príslušné orgány, aby vydávali príkazy na odstránenie, a stanovuje sa požiadavka, aby poskytovatelia hostingových služieb odstránili obsah do jednej hodiny od prijatia príkazu na odstránenie. Takisto sa v ňom stanovujú minimálne prvky, ktoré by mali obsahovať príkazy na odstránenie, a postupy, na základe ktorých poskytovatelia hostingových služieb poskytujú spätnú väzbu orgánu, ktorý ich vydáva, a informujú tento orgán, ak nie je možné príkaz splniť, resp. ak je potrebné ďalšie objasnenie. Vyžaduje sa v ňom takisto, aby vydávajúci orgán informoval orgán, ktorý vykonáva dohľad nad proaktívnymi opatreniami členského štátu, pod ktorého právomoc poskytovateľ hostingových služieb patrí.

V článku 5 sa stanovuje požiadavka, aby poskytovatelia hostingových služieb prijali opatrenia na urýchlené posúdenie obsahu postúpeného na základe hlásenia buď od príslušného orgánu v členskom štáte, alebo od subjektu Únie, avšak bez toho, aby bola uložená povinnosť odstrániť nahlásený obsah, ako aj bez toho, aby boli stanovené konkrétne lehoty na prijatie príslušných krokov. Takisto sa v ňom stanovujú minimálne prvky, ktoré by tieto hlásenia mali obsahovať, a postupy, ktorými poskytovatelia hostingových služieb poskytujú vydávajúcemu orgánu spätnú väzbu a ktorými žiadajú tento orgán o ozrejmenie.

V článku 6 sa vyžaduje, aby poskytovatelia hostingových služieb prijali účinné a primerané proaktívne opatrenia tam, kde je to vhodné. Stanovuje sa v ňom postup, ktorým sa zabezpečí, aby konkrétni poskytovatelia hostingových služieb (t. j. tí, ktorým bol určený konečný príkaz

na odstránenie) prijali v prípade potreby dodatočné proaktívne opatrenia na zmiernenie rizík v súlade s úrovňou vystavenia ich služieb teroristickému obsahu. Poskytovateľ hostingových služieb by mal spolupracovať s príslušným orgánom, pokiaľ ide o potrebné požadované opatrenia, a ak nie je možné dosiahnuť dohodu, môže orgán poskytovateľovi služieb opatrenia uložiť. V tomto článku sa stanovuje aj postup preskúmania rozhodnutia orgánu.

V článku 7 sa vyžaduje, aby poskytovatelia hostingových služieb uchovávali odstraňovaný obsah a súvisiace údaje počas šiestich mesiacov na účely preskúmacieho konania a na vyšetrovacie účely. Toto obdobie sa môže predĺžiť s cieľom umožniť ukončenie preskúmania. V článku sa takisto vyžaduje, aby poskytovatelia služieb zaviedli záruky, aby sa zabezpečilo, že uchovaný obsah a súvisiace údaje nie sú k dispozícii ani sa nespracúvajú na iné účely.

V článku 8 sa stanovuje povinnosť, aby poskytovatelia hostingových služieb vysvetlili svoje politiky zamerané na teroristický obsah a uverejňovali výročné správy na účely transparentnosti o opatreniach prijatých v tejto súvislosti.

V článku 9 sa stanovujú osobitné záruky, pokiaľ ide o používanie a vykonávanie proaktívnych opatrení v prípade využívania automatizovaných nástrojov, aby sa zabezpečilo, že rozhodnutia budú presné a podložené.

V článku 10 sa požaduje od poskytovateľov hostingových služieb, aby zaviedli mechanizmy na vybavovanie sťažností v súvislosti s odstraňovaním obsahu, hláseniami a proaktívnymi opatreniami a aby urýchlene preskúmali každú sťažnosť.

V článku 11 sa stanovuje povinnosť poskytovateľov hostingových služieb sprístupňovať informácie o odstránení poskytovateľom obsahu, pokiaľ príslušný orgán z dôvodov verejnej bezpečnosti nepožiadal o ich nesprístupnenie.

V článku 12 sa členským štátom ukladá povinnosť zabezpečiť, aby príslušné orgány mali dostatočné kapacity a zdroje na účely plnenia svojich povinností vyplývajúcich z tohto nariadenia.

V článku 13 sa vyžaduje, aby členské štáty spolupracovali medzi sebou a v prípade potreby aj s Europolom, s cieľom predísť duplicite a zásahom do vyšetrovaní. V tomto článku sa tiež stanovuje možnosť, aby členské štáty a poskytovatelia hostingových služieb využívali na spracovanie a spätnú väzbu v súvislosti s príkazmi na odstránenie a hláseniami vyhradené nástroje vrátane nástrojov Europolu, a spolupracovali na proaktívnych opatreniach. Takisto sa v ňom vyžaduje, aby členské štáty mali zavedené vhodné komunikačné kanály na zabezpečenie včasnej výmeny informácií pri vykonávaní a presadzovaní ustanovení podľa tohto nariadenia. Tento článok zaväzuje poskytovateľov hostingových služieb informovať príslušné orgány, ak sú si vedomí akéhokoľvek dôkazu o teroristických trestných činoch v zmysle článku 3 smernice (EÚ) 2017/541 o boji proti terorizmu .

V článku 14 sa stanovuje vytvorenie kontaktných miest zo strany poskytovateľov hostingových služieb, ako aj zo strany členských štátov s cieľom uľahčiť vzájomnú komunikáciu, a to najmä pokiaľ ide o hlásenia a príkazy na odstránenie.

V článku 15 sa stanovuje právomoc členského štátu na účely vykonávania dohľadu nad proaktívnymi opatreniami, stanovovania sankcií a monitorovania vyvíjaného úsilia.

V článku 16 sa vyžaduje, aby poskytovatelia hostingových služieb, ktorí nemajú sídlo v žiadnom z členských štátov, ale ktorí ponúkajú svoje služby v rámci Únie, určili v Únii právneho zástupcu.

V článku 17 sa od členských štátov vyžaduje, aby určili orgány príslušné na vydávanie príkazov na odstránenie, na hlásenie teroristického obsahu, na dohľad nad uplatňovaním proaktívnych opatrení a na presadzovanie tohto nariadenia.

V článku 18 sa stanovuje, že členské štáty by mali stanoviť pravidlá týkajúce sa sankcií za nesúlad a stanoviť kritériá, ktoré musia členské štáty zohľadniť pri určovaní druhu a úrovne týchto sankcií. So zreteľom na osobitný význam rýchleho odstránenia teroristického obsahu určeného v príkaze na odstránenie by sa mali zaviesť osobitné pravidlá, pokiaľ ide o finančné sankcie za systematické porušovanie tejto požiadavky.

V článku 19 sa stanovuje rýchlejší a pružnejší postup pri zmene vzorov formulárov príkazov na odstránenie a autentifikovaných kanálov na predkladanie písomností prostredníctvom delegovaných aktov.

V článku 20 sa stanovujú podmienky, za ktorých má Komisia právomoc prijímať delegované akty s cieľom stanoviť potrebné zmeny formulárov a technických požiadaviek na príkazy na odstránenie.

V článku 21 sa od členských štátov vyžaduje, aby zhromažďovali a oznamovali špecifické informácie týkajúce sa uplatňovania nariadenia s cieľom pomôcť Komisii pri výkone jej povinností podľa článku 23. Komisia stanoví podrobný program na monitorovanie výstupov, výsledkov a vplyvov tohto nariadenia.

V článku 22 sa stanovuje, že Komisia podá správu o vykonávaní tohto nariadenia dva roky po nadobudnutí jeho účinnosti.

V článku 23 sa stanovuje, že Komisia podá správu o hodnotení tohto nariadenia najskôr tri roky po nadobudnutí jeho účinnosti.

V článku 24 sa stanovuje, že navrhované nariadenie nadobudne účinnosť dvadsiatym dňom po jeho uverejnení v Úradnom vestníku EÚ a začne sa uplatňovať 6 mesiacov po dátume nadobudnutia jeho účinnosti. Táto lehota sa navrhuje, keďže budú potrebné vykonávacie nariadenia, no súčasne sa zohľadňuje aj naliehavosť úplného uplatňovania pravidiel navrhovaného nariadenia. Táto šesťmesačná lehota sa stanovila na základe predpokladu, že rokovania budú napredovať rýchlo.

2018/0331 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o predchádzaní šíreniu teroristického obsahu online

Príspevok Európskej komisie k stretnutiu čelných predstaviteľov v Salzburgu, 19. až 20. septembra 2018

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[6],

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.

(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

[6] Ú. v. EÚ C […], […], s. […].

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[7], 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.

(5) Uplatňovanie tohto nariadenia by nemalo mať vplyv na uplatňovanie článku 14 smernice 2000/31/ES[8]. Predovšetkým by žiadne opatrenia, ktoré prijal poskytovateľ hostingových služieb v súlade s týmto nariadením, vrátane akýchkoľvek proaktívnych opatrení, nemali samé o sebe 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.

(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.

(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, čo sú jedny zo základných pilierov 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.

---

[7] 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).

[8] 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).

(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 služieb a poskytovateľov obsahu účinne namietať proti príkazom na odstránenie na súde členského štátu, ktorého orgány toto rozhodnutie vydali.

(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[9]. So zreteľom na potrebu riešiť najškodlivejšiu teroristickú propagandu online by sa do tohto vymedzenia mal zahrnúť materiál a informácie, ktoré nabádajú na páchanie teroristických trestných činov alebo na poskytnutie pomoci pri páchaní týchto činov, resp. na ne motivujú alebo ich ospravedlňujú, ako aj ktoré predstavujú pokyny na páchanie takýchto trestných činov alebo ktoré podporujú účasť na činnostiach teroristickej skupiny. Medzi takéto informácie môže patriť 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 šírený na účely vzdelávania, novinárstva alebo výskumu by mal byť primerane chránený. Okrem toho by sa vyjadrovanie radikálnych, polemických alebo kontroverzných názorov vo verejnej diskusii o citlivých politických otázkach nemalo považovať za teroristický obsah.

(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 poskytované príjemcom služby na jeho žiadosť a ktoré sprístupňujú tieto uchovávané informácie tretím stranám, a to bez ohľadu na to, či je táto činnosť čisto technickej, automatickej alebo pasívnej povahy. Medzi takýchto poskytovateľov služieb informačnej spoločnosti patria napr. platformy sociálnych médií, služby na video prenos, služby na zdieľanie videí, obrazových a zvukových materiálov, služby na zdieľanie súborov a iné cloudové služby, a to v rozsahu, v akom sprístupňujú informácie tretím stranám a webovým lokalitám, na ktorých môžu používatelia umiestňovať svoje komentáre alebo príspevky. 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

[9] 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).

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[10]. Na druhej strane, poskytovanie služby výlučne len v záujme dodržiavania zákazu diskriminácie stanoveného v nariadení Európskeho parlamentu a Rady (EÚ) 2018/302[11], sa samo o sebe nemôže považovať za smerovanie činnosti do daného územia v rámci Únie, alebo zameranie sa na toto územie.

(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 teroristický. 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,

---

[10] 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).

[11] 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 menia nariadenia (ES) č. 2006/2004 a (EÚ) 2017/2394 a smernica 2009/22/ (Ú. v. EÚ L 601, 2.3.2018, s. 1).

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. Je na rozhodnutí poskytovateľov hostingových služieb, či príslušný obsah odstránia, alebo či k nemu znemožnia prístup pre používateľov v Únii.

(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 [12].

(15) Hlásenia príslušných orgánov alebo Europolu predstavujú účinný a rýchly prostriedok na zabezpečenie toho, aby poskytovatelia hostingových služieb získali vedomosť o konkrétnom obsahu svojich služieb. Tento mechanizmus upozornenia poskytovateľov hostingových služieb na informácie, ktoré sa môžu považovať za teroristický obsah, aby ho poskytovateľ dobrovoľne posúdil z hľadiska zlučiteľnosti so svojimi vlastnými podmienkami, by mal popri príkazoch na odstránenie zostať k dispozícii. 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) č. 2016/794[13] 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 nízkej úrovne vystavenia teroristickému obsahu.

---

[12] 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).

[13] 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 totožnosti poskytovateľa obsahu, ako aj údajov o prístupe, napríklad údaje o dátume a čase použitia poskytovateľa obsahu alebo o prihlásení do služby a odhlásení zo služby, spolu s IP adresou, ktorú poskytovateľovi obsahu pridelil poskytovateľ služby prístupu k internetu.

(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 predtým, 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 by mali uverejňovať výročné správy na účely transparentnosti obsahujúce užitočné informácie o opatreniach prijatých v súvislosti s odhaľovaním, identifikáciou a odstraňovaním teroristického obsahu.

(25) Postupy podávania sťažností predstavujú nevyhnutnú záruku pred chybným odstránením 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.

(26) Účinná právna ochrana podľa článku 19 Zmluvy o EÚ a článku 47 Charty základných práv Európskej únie si 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, pri vydávaní príkazov na odstránenie alebo zasielaní hlásení poskytovateľom hostingových služieb. 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.

(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, môžu členské štáty využiť 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[14].

(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, ktorý umožní elektronické predkladanie príkazov na odstránenie a hlásení, a z technických a 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 poskytovatelia hostingových služieb mali 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 svoje hlavné miesto podnikateľskej činnosti alebo v ktorom určil svojho právneho zástupcu. Ak však príkaz na odstránenie vydá iný členský štát, jeho orgány by mali mať možnosť presadzovať svoje príkazy prostredníctvom donucovacích opatrení nerepresívnej povahy, ako sú napr. peňažné sankcie. Pokiaľ ide o poskytovateľa hostingových služieb, ktorý nemá v Únii žiadnu prevádzkareň a neurčil právneho zástupcu, možnosť uložiť sankcie by mal mať každý členský štát, pod podmienkou dodržania zásady *ne bis in idem*.

[14] 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.

(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 upravujúce sankcie, a v prípade potreby aj usmernenia o ukladaní týchto sankcií. 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 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[15]. 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. Na účely hodnotenia právnych predpisov by sa mal vypracovať podrobný program monitorovania výstupov, výsledkov a vplyvov tohto nariadenia.

(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

[15] Ú. v. EÚ L 123, 12.5.2016, s.

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.

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:

   a) usadenie poskytovateľa hostingových služieb v Únii;

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

   c) zameranie činností na jeden alebo viac členských štátov;

4. „teroristické trestné činy“ sú trestné činy vymedzené v článku 3 ods. 1 smernice (EÚ) 2017/541;

5. „teroristický obsah“ je jedna alebo viacero z týchto informácií:

   a) podnecovanie na spáchanie teroristických trestných činov, resp. ich obhajovanie, a to aj ich glorifikáciou, v dôsledku ktorého vzniká nebezpečenstvo spáchania týchto činov;

   b) podpora prispievania k teroristickým trestným činom;

   c) podpora činností teroristickej skupiny, a to najmä podporovaním účasti na teroristickej skupine alebo jej podporou v zmysle článku 2 ods. 3 smernice (EÚ) 2017/541;

   d) 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.

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 na predchádzanie šíreniu teroristického obsahu, a tieto podmienky uplatnia.

Článok 4
Príkazy na odstránenie

1. Príslušný orgán má právomoc vydať rozhodnutie, 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;

   b) odôvodnenie, v ktorom sa vysvetľuje, prečo sa obsah považuje za teroristický, a to prinajmenšom vo forme odkazu na kategórie teroristického obsahu uvedené v článku 2 ods. 5;

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

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

   e) dátum a časovú pečiatku vydaného príkazu na odstránenie;

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

   g) 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 podrobné odôvodnenie, 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 potvrdia prijatie a bez zbytočného odkladu 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 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 dostatočne podrobné informácie vrátane dôvodov, prečo sa určitý obsah považuje za teroristický, 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 urýchlene 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 v prípade potreby prijmú 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) zabrániť opätovnému nahratiu 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. 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
Povinnosti 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 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 zabránenia opätovnému nahratiu 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 bezodkladne 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 [štyri] týždne od prijatia predmetného rozhodnutia. 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), 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. Členské štáty a poskytovatelia hostingových služieb sa môžu rozhodnúť, že použijú špecializované nástroje, a to v prípade potreby aj nástroje vytvorené 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 príslušnom členskom štáte alebo kontaktné miesto v členskom štáte podľa článku 14 ods. 2, podľa toho, kde majú svoje hlavné miesto podnikateľskej činnosti alebo svojho právneho zástupcu. Poskytovatelia hostingových služieb môžu v prípade pochybností poskytnúť tieto informácie Europolu, aby podnikol primerané nadväzujúce opatrenia.

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.

2. Ak poskytovateľ hostingových služieb neurčí právneho zástupcu, majú právomoc všetky členské štáty.

3. Ak orgán iného členského štátu vydal príkaz na odstránenie podľa článku 4 ods. 1, tento členský štát má právomoc prijať donucovacie opatrenia podľa svojho vnútroštátneho práva s cieľom vykonať tento príkaz na odstránenie.

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 príslušné orgány uvedené v odseku 1 najneskôr [*šesť 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 [*do šiestich 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 osoba;

d) finančnej sily zodpovednej právnickej 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. Právomoc prijímať delegované akty sa Komisii udeľuje 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 v ňom uvedenej. 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 [6 mesiacov od nadobudnutia účinnosti].

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

V Bruseli

Za Európsky parlament	*Za Radu*
predseda	*predseda*