NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2021/784

z 29. apríla 2021

o riešení šírenia teroristického obsahu online

(Text s významom pre EHP)

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

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

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

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

konajúc v súlade s riadnym legislatívnym postupom ([2]),

keďže:

(1) Cieľom tohto nariadenia je zabezpečiť hladké fungovanie digitálneho jednotného trhu v otvorenej a demokratickej spoločnosti tým, že sa bude riešiť zneužívanie hostingových služieb na teroristické účely a prispievať k verejnej bezpečnosti v Únii. Fungovanie digitálneho jednotného trhu by sa malo zlepšiť posilnením právnej istoty pre poskytovateľov hostingových služieb a dôvery používateľov v online prostredie, ako aj posilnením záruk v súvislosti so slobodou prejavu vrátane slobody prijímať a šíriť informácie a myšlienky v otvorenej a demokratickej spoločnosti a v súvislosti so slobodou a pluralitou médií.

(2) Regulačné opatrenia na riešenie šírenia teroristického obsahu online by sa mali doplniť stratégiami členských štátov na riešenie terorizmu, vrátane posilnenie mediálnej gramotnosti a kritického myslenia, vytvorenia alternatívnej argumentácie a protiargumentácie a inými iniciatívami na zníženie vplyvu teroristického obsahu online a zraniteľnosti voči nemu, ako aj investíciami do sociálnej práce, iniciatívami v oblasti deradikalizácie a spoluprácou s dotknutými komunitami s cieľom udržateľne predchádzať radikalizácii v spoločnosti.

(3) Riešenie teroristického obsahu online, ktorý je súčasťou širšieho problému nezákonného obsahu online si vyžaduje kombináciu legislatívnych, nelegislatívnych a dobrovoľných opatrení založených na spolupráci medzi orgánmi a poskytovateľmi hostingových služieb pri plnom rešpektovaní základných práv.

(4) 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, čím významnou mierou prispievajú k inovácii, hospodárskemu rastu a tvorbe pracovných miest v Únii. Služby poskytovateľov hostingových služieb sú však v určitých prípadoch zneužívané tretími stranami na účely protiprávneho konania online. Osobitné obavy vyvoláva zneužívanie týchto služieb zo strany teroristických skupín a ich podporovateľov na šírenie teroristického obsahu online s cieľom rozšíriť ich posolstvo, radikalizovať a uskutočniť nábor priaznivcov, ako aj na uľahčenie a riadenie teroristickej činnosti.

([1]) Ú. v. EÚ C 110, 22.3.2019, s. 67.

([2]) Pozícia Európskeho parlamentu zo 17. apríla 2019 (zatiaľ neuverejnená v úradnom vestníku) a pozícia Rady v prvom čítaní zo 16. marca 2021 (Ú. v. EÚ C 135, 16.4.2021, s. 1). Pozícia Európskeho parlamentu z 28. apríla 2021. (zatiaľ neuverejnená v úradnom vestníku).

(5) Prítomnosť teroristického obsahu online síce nie je jediným faktorom, no potvrdila sa ako katalyzátor radikalizácie jednotlivcov, ktorá môže viesť k teroristickým činom, a preto má vážne negatívne dôsledky pre používateľov, občanov a spoločnosť ako celok, ako aj pre poskytovateľov online služieb, ktorí sú hostiteľmi takéhoto obsahu, pretože podkopáva dôveru ich používateľov a poškodzuje ich obchodné modely. Vzhľadom na svoju ústrednú úlohu, ako aj technologické prostriedky a spôsobilosti spojené so službami, ktoré poskytujú, nesú poskytovatelia hostingových služieb osobitnú spoločenskú zodpovednosť za ochranu svojich služieb pred zneužitím zo strany teroristov a za poskytovanie pomoci pri riešení teroristického obsahu šíreného prostredníctvom ich služieb online, pričom sa zohľadňuje zásadný význam slobody prejavu vrátane slobody prijímať a šíriť informácie a myšlienky v otvorenej a demokratickej spoločnosti.

(6) Úsilie na úrovni Únie zamerané na boj proti teroristickému obsahu online sa začalo v roku 2015 prostredníctvom dobrovoľnej spolupráce medzi členskými štátmi a poskytovateľmi hostingových služieb. Toto úsilie treba doplniť jasným legislatívnym rámcom s cieľom ďalej znižovať prístup k teroristickému obsahu online a primerane reagovať na rýchlo sa vyvíjajúci problém. Legislatívny rámec stavia na dobrovoľnom úsilí, ktoré sa posilnilo odporúčaním Komisie (EÚ) 2018/334 ([3]), a reaguje na výzvy Európskeho parlamentu, aby sa v súlade s horizontálnym rámcom vytvoreným smernicou Európskeho parlamentu a Rady 2000/31/ES ([4]) posilnili opatrenia na riešenie nezákonného a škodlivého obsahu online, ako aj na výzvy Európskej rady, aby sa zlepšilo odhaľovanie a odstraňovanie obsahu online, ktorý podnecuje k teroristickým činom.

(7) Týmto nariadením by nemalo byť dotknuté uplatňovanie smernice 2000/31/ES. Predovšetkým by žiadne opatrenia, ktoré poskytovateľ hostingových služieb prijme v súlade s týmto nariadením, vrátane akýchkoľvek osobitných opatrení, nemali samy osebe viesť k tomu, že tento poskytovateľ hostingových služieb príde o výhodu výnimky zo zodpovednosti podľa uvedenej smernice. Toto nariadenie nemá vplyv ani na právomoci vnútroštátnych orgánov a súdov, pokiaľ ide o zodpovednosť poskytovateľov hostingových služieb v prípadoch, keď nie sú splnené podmienky stanovené v uvedenej smernici zakladajúce výnimku zo zodpovednosti.

(8) V prípade rozporu medzi týmto nariadením a smernicou Európskeho parlamentu a Rady 2010/13/EÚ ([5]), pokiaľ ide o ustanovenia upravujúce audiovizuálne mediálne služby v zmysle článku 1 ods. 1 písm. a) uvedenej smernice, by mala mať prednosť smernica 2010/13/EÚ. Tým by nemali byť dotknuté povinnosti podľa tohto nariadenia, a to najmä v súvislosti s poskytovateľmi platformy na zdieľanie videí.

(9) V tomto nariadení by sa mali stanoviť pravidlá zamerané na riešenie zneužívania hostingových služieb na šírenie teroristického obsahu online s cieľom zaručiť bezproblémové fungovanie vnútorného trhu. Uvedené pravidlá by mali plne rešpektovať základné práva, ktoré sú chránené v Únii, a najmä tie, ktoré sú zaručené Chartou základných práv Európskej únie (ďalej len „charta“).

(10) Toto nariadenie má prispievať k ochrane verejnej bezpečnosti a zároveň vytvárať primerané a spoľahlivé záruky na zabezpečenie ochrany základných práv vrátane práva na rešpektovanie súkromného života, na ochranu osobných údajov, na slobodu prejavu vrátane slobody prijímať a šíriť informácie, ako aj slobodu podnikania a na účinný prostriedok nápravy. Navyše je zakázaná aj akákoľvek diskriminácia. 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, a sloboda a pluralita médií, ktoré sú základnými piliermi pluralistickej a demokratickej spoločnosti a hodnotami, na ktorých je Únia založená. Opatrenia, ktoré ovplyvňujú slobodu prejavu a právo na informácie, by mali byť presne zamerané na riešenie šírenia teroristického obsahu online, a to pri rešpektovaní práva prijímať a šíriť informácie zákonným spôsobom, pri zohľadnení ústrednej úlohy poskytovateľov hostingových služieb pri uľahčovaní verejnej diskusie a prijímaní a šírení faktov, názorov a myšlienok v súlade s právom. Účinné online opatrenia na riešenie teroristického obsahu online a ochrana slobody prejavu a práva na informácie nie sú protichodné ciele, ale ciele, ktoré sa dopĺňajú a vzájomne posilňujú.

([3]) 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).

([4]) 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).

([5]) Smernica Európskeho parlamentu a Rady 2010/13/EÚ z 10. marca 2010 o koordinácii niektorých ustanovení upravených zákonom, iným právnym predpisom alebo správnym opatrením v členských štátoch týkajúcich sa poskytovania audiovizuálnych mediálnych služieb (smernica o audiovizuálnych mediálnych službách) (Ú. v. EÚ L 95, 15.4.2010, s. 1).

(11) V záujme ozrejmenia opatrení, ktoré majú prijať poskytovatelia hostingových služieb a príslušné orgány s cieľom riešiť šírenie teroristického obsahu online, by sa v tomto nariadení malo stanoviť vymedzenie teroristického obsahu na preventívne účely, ktoré by bolo v súlade s vymedzením príslušných trestných činov podľa smernice Európskeho parlamentu a Rady (EÚ) 2017/541 ([6]). Vzhľadom na potrebu riešiť najškodlivejšiu teroristickú propagandu online by sa do tohto vymedzenia mal zahrnúť materiál, ktorý niekoho podnecuje alebo navádza na páchanie trestných činov terorizmu alebo poskytnutie pomoci pri páchaní týchto činov, niekoho navádza na účasť na činnostiach teroristickej skupiny, alebo glorifikuje teroristické činnosti, vrátane materiálu, ktorý zobrazuje teroristický útok. Okrem toho by toto vymedzenie malo zahŕňať aj materiál, ktorý poskytuje inštrukcie na výrobu alebo používanie výbušnín, strelných zbraní alebo iných zbraní, alebo škodlivých alebo nebezpečných látok, ako aj chemických, biologických, rádiologických a jadrových látok (CBRN), či iných osobitných metód alebo techník vrátane výberu cieľov na účely spáchania trestných činov terorizmu alebo poskytnutia pomoci pri páchaní takýchto činov. Takýto materiál zahŕňa texty, obrázky, zvukové záznamy a videá, ako aj živé vysielanie trestných činov terorizmu, čím spôsobuje nebezpečenstvo ďalšieho páchania takýchto trestných činov. Pri posudzovaní toho, či materiál predstavuje teroristický obsah v zmysle tohto nariadenia, by príslušné orgány a poskytovatelia hostingových služieb mali zohľadniť také faktory, ako je napríklad povaha a znenie vyhlásení, kontext, v ktorom boli tieto vyhlásenia urobené, ako aj ich potenciál viesť ku škodlivým následkom s vplyvom na bezpečnosť a ochranu osôb. Významným faktorom pri posudzovaní by mala byť skutočnosť, že materiál vyrobila osoba, skupina alebo subjekt zahrnuté do zoznamu osôb, skupín alebo subjektov zapojených do teroristických činov, a na ktoré sa vzťahujú reštriktívne opatrenia, alebo že je materiál tejto osobe, skupine alebo subjektu pripísateľný alebo šírený v mene takejto osoby, skupiny alebo subjektu.

(12) Materiál šírený na vzdelávacie, novinárske, umelecké alebo výskumné účely alebo na účely zvyšovania povedomia v záujme boja proti teroristickej činnosti by sa nemal považovať za teroristický obsah. Pri určovaní toho, či materiál, ktorý poskytuje poskytovateľ obsahu, predstavuje „teroristický obsah“ vymedzený v tomto nariadení, by sa mala zohľadniť najmä sloboda prejavu a právo na informácie, vrátane slobody a plurality médií a slobody umenia a vedeckého bádania. Najmä v prípadoch, keď poskytovateľ obsahu nesie redakčnú zodpovednosť, by sa pri každom rozhodovaní o odstránení šíreného materiálu mali zohľadňovať novinárske normy stanovené predpismi pre tlač alebo médiá v súlade s právom Únie vrátane charty. Okrem toho by sa vyjadrovanie radikálnych, polemických alebo kontroverzných názorov vo verejnej diskusii o citlivých politických otázkach nemalo považovať za teroristický obsah.

(13) S cieľom účinne riešiť šírenie teroristického obsahu online a zároveň zabezpečiť rešpektovanie súkromného života jednotlivcov by sa toto nariadenie malo uplatňovať na poskytovateľov služieb informačnej spoločnosti, ktorí na žiadosť používateľa týchto služieb uchovávajú a verejne šíria informácie a materiál, ktoré poskytol, a to bez ohľadu na to, či je uchovávanie a verejné šírenie takýchto informácií a materiálu čisto technickej, automatickej a pasívnej povahy. Pojem „uchovávanie“ by sa mal chápať ako uchovávanie údajov v pamäti fyzického alebo virtuálneho servera. Poskytovatelia služieb „iba prenos“ („mere conduit“) alebo „ukladanie informácií v pamäti“ („caching“), ako aj iných služieb poskytovaných na iných úrovniach internetovej infraštruktúry, ktoré nezahŕňajú uchovávanie, ako sú správcovia doménových mien a registrátori, ako aj poskytovatelia systémov doménových mien (DNS) a služieb ochrany platieb alebo ochrany pred distribuovanými útokmi na vyradenie služby (DDoS) by preto nemali patriť do rozsahu pôsobnosti tohto nariadenia.

(14) Pojem „verejné šírenie“ by mal zahŕňať sprístupňovanie informácií potenciálne neobmedzenému počtu osôb, a to zabezpečenie jednoduchého prístupu k informáciám pre používateľov vo všeobecnosti bez toho, aby sa vyžadoval ďalší zásah poskytovateľa obsahu, a bez ohľadu na to, či dané osoby skutočne využijú prístup k predmetným informáciám. Preto, ak si prístup k informáciám vyžaduje registráciu alebo udelenie prístupu do skupiny používateľov, mali by sa informácie považovať za verejne šírené len vtedy, ak registrácia alebo udelenie prístupu pre používateľov, ktorí chcú získať prístup k daným informáciám, prebieha automaticky bez toho, aby rozhodnutie alebo výber, komu sa udelí prístup, robil človek. Interpersonálne komunikačné služby vymedzené v článku 2 bode 5 smernice Európskeho parlamentu a Rady (EÚ) 2018/1972 ([7]), ako sú e-maily alebo služby zasielania súkromných správ, by nemali patriť do rozsahu pôsobnosti tohto nariadenia. Informácie by sa mali považovať za uchovávané

([6]) 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).

([7]) Smernica Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií (Ú. v. EÚ L 321, 17.12.2018, s. 36).

a verejne šírené v zmysle tohto nariadenia len vtedy, ak sa takéto činnosti vykonávajú na priamu žiadosť poskytovateľa obsahu. V dôsledku toho by sa toto nariadenie nemalo vzťahovať na poskytovateľov služieb, ako je napríklad cloudová infraštruktúra, ktoré sa poskytujú na žiadosť iných strán, než sú poskytovatelia obsahu, a z ktorých majú poskytovatelia obsahu len nepriamy prospech. Toto nariadenie by sa malo vzťahovať napríklad na poskytovateľov sociálnych médií, služieb zameraných na zdieľanie videí, fotografií a zvukových záznamov, ako aj služieb zameraných na zdieľanie súborov a iných cloudových služieb, pokiaľ sa tieto služby využívajú na sprístupnenie uchovávaných informácií verejnosti na základe priamej žiadosti poskytovateľa obsahu. Ak poskytovateľ hostingových služieb ponúka viacero služieb, toto nariadenie by sa malo uplatňovať len v súvislosti so službami, ktoré patria do jeho rozsahu pôsobnosti.

(15) Teroristický obsah sa často verejne šíri prostredníctvom služieb poskytovaných poskytovateľmi hostingových služieb usadenými v tretích krajinách. S cieľom chrániť používateľov v Únii a zabezpečiť, aby všetci poskytovatelia hostingových služieb pôsobiaci na digitálnom jednotnom trhu podliehali rovnakým požiadavkám, by sa toto nariadenie malo uplatňovať na všetkých poskytovateľov relevantných služieb ponúkaných v Únii bez ohľadu na krajinu ich hlavného miesta podnikateľskej činnosti. Poskytovateľ hostingových služieb sa považuje za ponúkajúceho služby v Únii, ak umožňuje fyzickým alebo právnickým osobám v jednom alebo viacerých členských štátoch využívať svoje služby a má podstatnú väzbu na daný členský štát alebo členské štáty.

(16) Podstatná väzba s Úniou existuje, ak má poskytovateľ hostingových služieb miesto podnikateľskej činnosti v Únii, ak používa jeho služby významný počet používateľov v jednom alebo vo viacerých členských štátoch alebo keď sa jeho činnosti zameriavajú na jeden alebo viacero členských štátov. Zameranie činností na jeden alebo viac členských štátov by sa malo určiť na základe všetkých relevantných okolností vrátane takých faktorov, ako je napríklad používanie jazyka alebo meny, ktoré sa všeobecne používajú v dotknutom členskom štáte, alebo na základe možnosti objednávania tovaru alebo služieb z takého členského štátu. Takéto zameranie by sa mohlo odvodiť aj z dostupnosti aplikácie v príslušnom vnútroštátnom obchode s aplikáciami, z poskytovania miestnej reklamy alebo reklamy v jazyku všeobecne používanom v dotknutom členskom štáte, alebo z prístupu ku vzťahom so zákazníkmi, ako je napríklad poskytovanie služieb zákazníkom v jazyku všeobecne používanom v danom členskom štáte. Za podstatnú väzbu by sa mal považovať aj prípad, keď poskytovateľ hostingových 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 (EÚ) č. 1215/2012 ([8]). Samotná prístupnosť webového sídla poskytovateľa hostingových služieb, e-mailovej adresy, alebo iných kontaktných údajov v jednom alebo viacerých členských štátoch by však sama osebe nemala dostatočne predstavovať podstatnú väzbu. Navyše poskytovanie služby výlučne len v záujme dodržiavania zákazu diskriminácie stanoveného v nariadení Európskeho parlamentu a Rady (EÚ) 2018/302 ([9]) by sa samo osebe nemalo považovať za podstatnú väzbu k Únii.

(17) Mali by sa zosúladiť postupy a povinnosti vyplývajúce z príkazov na odstránenie vydaných na základe posúdenia príslušnými orgánmi, ktorými sa poskytovateľom hostingových služieb ukladá povinnosť odstrániť teroristický obsah alebo znemožniť prístup k nemu. Vzhľadom na rýchlosť, akou sa šíri teroristický obsah v rámci online služieb, mala by sa uložiť povinnosť poskytovateľom hostingových služieb zabezpečiť, aby sa teroristický obsah uvedený v príkaze na odstránenie odstránil alebo aby sa znemožnil prístup k nemu vo všetkých členských štátoch, a to do jednej hodiny od doručenia tohto príkazu. Okrem riadne odôvodnených naliehavých prípadov by mal príslušný orgán poskytnúť poskytovateľovi hostingových služieb informácie o postupoch a uplatniteľných lehotách aspoň 12 hodín vopred pred vydaním prvého príkazu na odstránenie danému poskytovateľovi hostingových služieb. O riadne odôvodnený naliehavý prípad ide vtedy, keď by odstránenie obsahu alebo znemožnenie prístupu k nemu neskôr ako jednu hodinu po doručení príkazu na odstránenie viedlo k vážnej ujme, napríklad v situáciách bezprostredného ohrozenia života alebo fyzickej integrity osoby alebo ak takýto obsah zobrazuje prebiehajúce udalosti, ktorých výsledkom je ujma na živote alebo fyzickej integrite osoby. Príslušný orgán by mal určiť, či prípady predstavujú naliehavé prípady a riadne odôvodniť svoje rozhodnutie v príkaze na odstránenie. V prípade, že poskytovateľ hostingových služieb nemôže splniť príkaz na odstránenie do jednej hodiny od jeho prijatia z dôvodu vyššej moci alebo faktických prekážok, vrátane objektívne odôvodniteľných technických alebo prevádzkových dôvodov, mal by o tom čo najskôr informovať vydávajúci príslušný orgán a príkaz na odstránenie splniť hneď, ako sa situácia vyrieši.

([8]) 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).

([9]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/302 z 28. februára 2018 o riešení neodôvodneného geografického blokovania a iných foriem diskriminácie z dôvodu štátnej príslušnosti, miesta bydliska alebo sídla zákazníkov na vnútornom trhu, ktorým sa mení nariadenia (ES) č. 2006/2004 a (EÚ) 2017/2394 a smernica 2009/22/ES (Ú. v. EÚ L 60 I, 2.3.2018, s. 1).

(18) Príkaz na odstránenie by mal uvádzať dôvody, na základe ktorých je materiál kvalifikovaný na odstránenie alebo na znemožnenie prístupu k jeho obsahu ako teroristickému obsahu a mal by poskytnúť dostatok informácií na lokalizáciu uvedeného obsahu, uvedením presnej URL a v prípade potreby akýchkoľvek ďalších informácií, ako sú napríklad snímky obrazovky s príslušným obsahom. Toto odôvodnenie by malo poskytovateľovi hostingových služieb a v konečnom dôsledku poskytovateľovi obsahu umožňovať účinné uplatnenie ich práva na súdny prostriedok nápravy. Poskytnuté odôvodnenie by nemalo obsahovať zverejnenie citlivých informácií, ktoré by mohli ohroziť prebiehajúce vyšetrovanie.

(19) Príslušný orgán by mal predložiť príkaz na odstránenie priamo na kontaktné miesto určené alebo zriadené poskytovateľom hostingových služieb na účely tohto nariadenia prostredníctvom akýchkoľvek elektronických prostriedkov, ktoré umožňujú vyhotoviť písomný záznam za takých podmienok, ktoré umožnia poskytovateľovi hostingových služieb overiť pravosť príkazu, vrátane presného dátumu a času odoslania a doručenia príkazu, napríklad prostredníctvom zabezpečeného e-mailu alebo platforiem alebo iných zabezpečených kanálov vrátane tých, ktoré poskytovateľ hostingových služieb poskytol v súlade s právom Únie na ochranu osobných údajov. Uvedenú požiadavku by malo byť možné splniť okrem iného využitím kvalifikovaných elektronických doručovacích služieb pre registrované zásielky v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 ([10]). Ak sa hlavné miesto podnikateľskej činnosti poskytovateľa hostingových služieb nachádza, alebo jeho právny zástupca má pobyt alebo je usadený, v inom členskom štáte, ako je členský štát vydávajúceho príslušného orgánu, kópia tohto príkazu na odstránenie by sa mala súčasne predložiť príslušnému orgánu daného členského štátu.

(20) Malo by byť možné, aby príslušný orgán členského štátu, v ktorom má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca, skontroloval príkaz na odstránenie vydaný príslušným orgánom iného členského štátu, aby zistil, či závažným alebo zjavným spôsobom neporušuje toto nariadenie alebo základné práva zakotvené v charte. Poskytovateľ obsahu, ako aj poskytovateľ hostingových služieb by mali mať právo požiadať o takúto kontrolu príslušným orgánom v členskom štáte, v ktorom má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca. V prípade takejto žiadosti by mal príslušný orgán prijať rozhodnutie o tom, či príkaz na odstránenie obsahuje takéto porušenie. Ak dané rozhodnutie zistí takéto porušenie, právne účinky príkazu na odstránenie by mali zaniknúť. Kontrola by mala prebehnúť rýchlo, aby sa čo najskôr zabezpečilo obnovenie chybne odstráneného obsahu alebo obsahu, ku ktorému bol znemožnený prístup.

(21) Poskytovatelia hostingových služieb vystavení teroristickému obsahu, ktorí stanovili svoje zmluvné podmienky, by do nich mali zahrnúť ustanovenia na riešenie zneužívania svojich služieb na verejné šírenie teroristického obsahu. Uvedené ustanovenia by mali uplatňovať dôsledne, transparentne, primerane a nediskriminačne.

(22) Vzhľadom na rozsah problému a rýchlosť potrebnú na účinnú identifikáciu a odstránenie teroristického obsahu, sú nevyhnutným prvkom pri riešení problému teroristického obsahu online účinné a primerané osobitné opatrenia. S cieľom znížiť dostupnosť teroristického obsahu vo svojich službách by poskytovatelia hostingových služieb vystavení teroristickému obsahu mali zaviesť osobitné opatrenia, pričom by mali zohľadniť riziká a úroveň vystavenia teroristickému obsahu, ako aj účinky na práva tretích strán a na verejný záujem na informovanie. Poskytovatelia hostingových služieb by mali určiť, aké vhodné, účinné a primerané osobitné opatrenia by sa mali zaviesť na identifikáciu a odstraňovanie teroristického obsahu. Osobitné opatrenia by mohli zahŕňať vhodné technické alebo operačné opatrenia alebo kapacity, ako napríklad personálne zabezpečenie alebo technické prostriedky na identifikáciu a rýchle odstránenie teroristického obsahu alebo znemožnenie prístupu k nemu, mechanizmy umožňujúce používateľom nahlasovať alebo označovať možný teroristický obsah alebo akékoľvek iné opatrenia, ktoré poskytovateľ hostingových služieb považuje za vhodné a účinné na riešenie dostupnosti teroristického obsahu v rámci svojich služieb.

(23) Poskytovatelia hostingových služieb by mali pri zavádzaní osobitných opatrení zabezpečiť, aby bolo zachované právo používateľov na slobodu prejavu a právo na informácie, ako aj sloboda a pluralita médií, ktoré chráni charta. Okrem požiadaviek stanovených v právnom poriadku vrátane právnych predpisov o ochrane osobných údajov by mali poskytovatelia hostingových služieb konať s náležitou starostlivosťou a v relevantných prípadoch uplatňovať záruky vrátane ľudského dohľadu a overovania, aby sa vyhli akémukoľvek neúmyselnému alebo nesprávnemu rozhodnutiu, ktoré by viedlo k odstráneniu obsahu, ktorý nie je teroristickým obsahom, alebo k znemožneniu prístupu k nemu.

([10]) 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).

(24) Poskytovateľ hostingových služieb by mal nahlásiť príslušnému orgánu osobitné opatrenia, ktoré zaviedol, aby príslušný orgán mohol určiť, či sú opatrenia účinné a primerané a či v prípade, že sa používajú automatizované prostriedky, má poskytovateľ hostingových služieb potrebné kapacity na manuálny dohľad a overovanie. Pri posudzovaní účinnosti a primeranosti opatrení by príslušné orgány mali zohľadniť relevantné parametre vrátane počtu príkazov na odstránenie, ktoré boli voči danému poskytovateľovi hostingových služieb vydané, veľkosť a ekonomické možnosti poskytovateľa hostingových služieb a vplyv jeho služieb na šírenie teroristického obsahu, napríklad na základe počtu používateľov v Únii, ako aj záruky zavedené s cieľom riešiť zneužívanie jeho služieb na šírenie teroristického obsahu online.

(25) Ak sa príslušný orgán domnieva, že zavedené osobitné opatrenia sú nedostatočné na riešenie rizík mal by mať možnosť požiadať o prijatie dodatočných vhodných, účinných a primeraných osobitných opatrení. Požiadavka na zavedenie takýchto osobitných opatrení by nemala viesť k všeobecnej povinnosti monitorovať alebo aktívne zisťovať skutočnosti alebo okolnosti v zmysle článku 15 ods. 1 smernice 2000/31/ES, ani k povinnosti používať automatizované nástroje. Poskytovatelia hostingových služieb by však mali mať možnosť používať automatizované nástroje, ak to považujú za vhodné a potrebné na účinné riešenie zneužívania svojich služieb na šírenie teroristického obsahu.

(26) Povinnosť poskytovateľov hostingových služieb uchovávať odstránený obsah a súvisiace údaje by sa mala stanoviť na osobitné účely a mala by platiť len počas nevyhnutne potrebného obdobia. Povinnosť uchovávania je nutné vztiahnuť aj na súvisiace údaje, a to v rozsahu, v akom by sa akékoľvek takéto údaje v dôsledku odstránenia predmetného teroristického obsahu inak stratili. Súvisiace údaje môžu zahŕňať údaje, ako sú údaje o účastníkovi, najmä údaje, ktoré sa týkajú totožnosti poskytovateľa obsahu, a údaje o prístupe vrátane údajov o dátume a čase použitia služby poskytovateľom obsahu a o prihlásení sa do nej a odhlásení sa z nej, spolu s IP adresou, ktorú poskytovateľovi obsahu pridelil poskytovateľ služby prístupu na internet.

(27) Povinnosť uchovávať obsah na účely správneho alebo súdneho preskúmania je nevyhnutná a opodstatnená z hľadiska potreby zabezpečiť, aby poskytovatelia obsahu, ktorých obsah bol odstránený alebo ku ktorému bol znemožnený prístup, mali účinné nápravné opatrenia ako aj s cieľom zabezpečiť obnovenie tohto obsahu, a to v závislosti od výsledku uvedených konaní. Povinnosť uchovávať materiál na účely vyšetrovania alebo trestného stíhania je odôvodnená a nevyhnutná so zreteľom na prínos, ktorý by tento materiál mohol mať v záujme narušenia teroristickej činnosti alebo jej predchádzania. Uchovávanie odstráneného teroristického obsahu na účely predchádzania trestným činom terorizmu a ich odhaľovania, vyšetrovania a stíhania by sa preto tiež malo považovať za odôvodnené. Teroristický obsah a súvisiace údaje by sa mali uchovávať iba na obdobie potrebné pre orgány presadzovania práva, aby mohli skontrolovať uvedený teroristický obsah a rozhodnúť, či bude potrebný na uvedené účely. Na účely predchádzania trestným činom terorizmu, ich odhaľovania, vyšetrovania a stíhania by sa požadované uchovávanie údajov malo obmedziť len na údaje, pri ktorých je pravdepodobné, že súvisia s trestnými činmi terorizmu, a mohli by preto prispieť k stíhaniu trestných činov terorizmu alebo k predchádzaniu závažným hrozbám pre verejnú bezpečnosť. Ak poskytovatelia hostingových služieb odstránia materiál alebo k nemu znemožnia prístup, najmä prostredníctvom vlastných osobitných opatrení, mali by bezodkladne informovať príslušné orgány o obsahu, ktorý obsahuje informácie, ktoré zahŕňajú bezprostredné ohrozeniu života alebo podozrenie zo spáchania trestného činu terorizmu.

(28) Aby sa zabezpečila proporcionalita, doba uchovávania by mala byť obmedzená na šesť mesiacov, aby poskytovatelia obsahu mali dostatočný čas na začatie správneho alebo súdneho preskúmania a aby sa orgánom presadzovania práva umožnil prístup k relevantným údajom na účely vyšetrovania a stíhania trestných činov terorizmu. Malo by však byť možné na žiadosť príslušného orgánu alebo súdu predĺžiť toto obdobie na tak dlho, ako je potrebné v prípadoch, ak sa uvedené konania začnú, ale neskončia do šiestich mesiacov. Trvanie obdobia uchovávania by malo postačovať na to, aby orgány presadzovania práva mohli uchovať potrebné materiály v súvislosti s vyšetrovaniami a stíhaniami a aby sa zároveň zabezpečila rovnováha v súvislosti so základnými právami.

(29) Týmto nariadením by nemali byť dotknuté procesné záruky ani procesné vyšetrovacie opatrenia, ktoré sa týkajú prístupu k obsahu a súvisiacim údajom uchovávaným na účely vyšetrovania a trestného stíhania trestných činov terorizmu, a ktoré sú upravené právom Únie alebo vnútroštátnym právom.

(30) 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 digitálny jednotný trh. Poskytovatelia hostingových služieb, ktorí v určitom kalendárnom roku podnikli alebo ktorým sa uložila povinnosť podniknúť kroky podľa tohto nariadenia, by mali uverejniť výročnú správu o transparentnosti obsahujúcu informácie o krokoch podniknutých v súvislosti s odhaľovaním, identifikáciou a odstraňovaním teroristického obsahu.

(31) Príslušné orgány by mali uverejňovať výročné správy o transparentnosti obsahujúce informácie o počte príkazov na odstránenie, počte prípadov, kedy nebol príkaz vykonaný, počte rozhodnutí o osobitných opatreniach, počte prípadov, ktoré sú predmetom správneho alebo súdneho preskúmania a počte rozhodnutí o uložení sankcií.

(32) Právo na účinný prostriedok nápravy je zakotvené v článku 19 Zmluvy o Európskej únii (ďalej len „Zmluva o EÚ“) a v článku 47 charty. Každá fyzická alebo právnická osoba má právo na účinný 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 by malo zahŕňať najmä možnosť poskytovateľov hostingových služieb a poskytovateľov obsahu účinne namietať proti príkazom na odstránenie alebo akýmkoľvek rozhodnutiam prijatým na základe kontroly príkazov na odstránenie podľa tohto nariadenia na súde členského štátu, ktorého príslušné orgány vydali príkaz na odstránenie alebo prijali rozhodnutie, ako aj možnosť poskytovateľov hostingových služieb účinne namietať proti rozhodnutiu, ktoré sa týka osobitných opatrení alebo sankcií, na súde členského štátu, ktorého príslušný orgán prijal dané rozhodnutie.

(33) Postupy podávania sťažností predstavujú potrebnú záruku, aby nedošlo k chybnému odstráneniu obsahu online alebo znemožneniu prístupu k nemu, ak je takýto obsah chránený 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. Požiadavkou, aby poskytovateľ hostingových služieb obnovil obsah, ktorý bol odstránený omylom alebo ku ktorému bol omylom znemožnený prístup, by nemala byť dotknutá možnosť poskytovateľov hostingových služieb presadzovať svoje vlastné zmluvné podmienky.

(34) Účinná právna ochrana v súlade s článkom 19 Zmluvy o EÚ a článkom 47 charty si vyžaduje, aby mali poskytovatelia obsahu možnosť zistiť dôvody, na základe ktorých bol obsah, ktorý poskytujú, odstránený, alebo na základe ktorých bol k nemu znemožnený prístup. Na tento účel by poskytovateľ hostingových služieb mal poskytnúť poskytovateľovi obsahu informácie, ktoré by poskytovateľovi obsahu umožňovali napadnúť odstránenie alebo znemožnenie prístupu. V závislosti od okolností by mohli poskytovatelia hostingových služieb nahradiť obsah, ktorý bol odstránený alebo ku ktorému bol znemožnený prístup, správou uvádzajúcou, že tento obsah bol odstránený alebo že prístup k tomu obsahu bol znemožnený v súlade s týmto nariadením. Na žiadosť poskytovateľa obsahu by sa mali poskytnúť ďalšie informácie o dôvodoch odstránenia alebo znemožnenia prístupu, ako aj o prostriedkoch nápravy voči odstráneniu alebo znemožneniu prístupu. Ak príslušné orgány rozhodnú, že z dôvodov verejnej bezpečnosti, a to aj v kontexte vyšetrovania, je nevhodné alebo kontraproduktívne, aby bol poskytovateľ obsahu priamo oboznámený s odstránením určitého obsahu alebo so znemožnením prístupu k nemu, mali by o tom zodpovedajúcim spôsobom informovať poskytovateľa hostingových služieb.

(35) Členské štáty by mali určiť príslušné orgány na účely tohto nariadenia. Toto by nemalo nutne znamenať zriadenie nového orgánu a malo by byť možné zveriť úlohy stanovené v tomto nariadení existujúcemu orgánu. V tomto nariadení by sa malo vyžadovať určenie orgánov príslušných na vydávanie príkazov na odstránenie, na kontrolu príkazov na odstránenie, na dohľad nad osobitnými opatreniami a na ukladanie sankcií, pričom by malo byť na každom členskom štáte, aby rozhodol o počte príslušných orgánov, ktoré sa majú určiť, a o tom, či to budú správne orgány, orgány presadzovania práva alebo justičné orgány. Členské štáty by mali zabezpečiť, aby si príslušné orgány plnili svoje úlohy objektívne a nediskriminačne a aby nežiadali ani neprijímali pokyny od žiadneho iného orgánu v súvislosti s plnením úloh podľa tohto nariadenia. Toto by nemalo brániť výkonu dohľadu podľa vnútroštátneho ústavného práva. Členské štáty by mali oznámiť príslušné orgány určené podľa tohto nariadenia Komisii, ktorá by mala uverejniť online register príslušných orgánov. Tento online register by mal byť ľahko prístupný, aby sa poskytovateľom hostingových služieb uľahčilo rýchle overovanie pravosti príkazov na odstránenie.

(36) S cieľom vyhnúť sa duplicite úsilia a možným zásahom do vyšetrovaní a minimalizovať zaťaženie dotknutých poskytovateľov hostingových služieb by sa pred vydaním príkazov na odstránenie mali príslušné orgány navzájom informovať, mali by koordinovať svoju činnosť a spolupracovať a v relevantných prípadoch by mali do týchto aktivít zapojiť Europol. Pri rozhodovaní o vydaní príkazu na odstránenie by mal príslušný orgán náležite zohľadniť každé oznámenie o zasahovaní do vyšetrovacích záujmov (predchádzanie konfliktu záujmov). Keď príslušný orgán dostane od príslušného orgánu z iného členského štátu informácie o existujúcom príkaze na odstránenie, nemal by vydať príkaz na odstránenie v rovnakej veci. Pokiaľ ide o vykonávanie ustanovení tohto nariadenia, Europol by mohol poskytovať podporu v súlade so svojím súčasným mandátom a existujúcim právnym rámcom.

(37) S cieľom zabezpečiť účinné a dostatočne koherentné vykonávanie osobitných opatrení prijatých poskytovateľmi hostingových služieb by mali príslušné orgány navzájom koordinovať svoju činnosť a spolupracovať v súvislosti s komunikáciou s poskytovateľmi hostingových služieb týkajúcou sa príkazov na odstránenie a určenia, vykonávania a posudzovania osobitných opatrení. Koordinácia a spolupráca je tiež potrebná v súvislosti s inými opatreniami na vykonávanie tohto nariadenia vrátane v súvislosti s prijímaním pravidiel o sankciách a ukladaním sankcií. Komisia by mala takúto koordináciu a spoluprácu uľahčovať.

(38) Je nevyhnutné, aby bol príslušný orgán členského štátu, ktorý je zodpovedný za ukladanie sankcií, v plnej miere informovaný o vydávaní príkazov na odstránenie, ako aj o následnej komunikácii medzi poskytovateľom hostingových služieb a príslušnými orgánmi v iných členských štátoch. Na tento účel by členské štáty mali zabezpečiť vhodné a zabezpečené komunikačné kanály a mechanizmy, ktoré umožnia včasnú výmenu relevantných informácií.

(39) S cieľom uľahčiť rýchlu komunikáciu medzi príslušnými orgánmi, ako aj s poskytovateľmi hostingových služieb a s cieľom zabrániť duplicite úsilia by sa mali členské štáty nabádať, aby využívali špecializované nástroje, ktoré vytvoril Europol, ako je súčasná aplikácia na správu nahlasovania internetového obsahu alebo nástroje, ktoré ju nahradia.

(40) Ukázalo sa, že nahlasovanie zo strany členských štátov a Europolu je účinným a rýchlym prostriedkom zvyšovania informovanosti poskytovateľov hostingových služieb o konkrétnom obsahu dostupnom v rámci ich služieb, ktorý im umožňuje rýchlo konať. Takéto nahlasovanie, ktoré je mechanizmom upozorňovania poskytovateľov hostingových služieb na informácie, ktoré by sa mohli považovať za teroristický obsah, aby ho poskytovateľ dobrovoľne posúdil z hľadiska zlučiteľnosti tohto obsahu s vlastnými zmluvnými podmienkami, by malo zostať k dispozícii popri príkazoch na odstránenie. Konečné rozhodnutie o tom, či odstrániť obsah z dôvodu nesúladu s jeho zmluvnými podmienkami, je na poskytovateľovi hostingových služieb. Týmto nariadením by nemal byť dotknutý mandát Europolu stanovený v nariadení Európskeho parlamentu a Rady (EÚ) 2016/794 ([11]). Žiadne ustanovenie tohto nariadenia by sa preto nemalo chápať tak, že členským štátom a Europolu bráni využívať nahlasovanie ako nástroj na riešenie teroristického obsahu online.

(41) Vzhľadom na konkrétne závažné dôsledky určitého teroristického obsahu online by poskytovatelia hostingových služieb mali bezodkladne informovať relevantné orgány v dotknutom členskom štáte alebo príslušné orgány v členskom štáte, v ktorom sú usadení alebo majú právneho zástupcu, o teroristickom obsahu, ktorý zahŕňa bezprostredné ohrozenie života alebo podozrenie zo spáchania trestného činu terorizmu. V záujme zabezpečenia proporcionality by sa táto povinnosť mala obmedziť len na trestné činy terorizmu vymedzené v článku 3 ods. 1 smernice (EÚ) 2017/541. Uvedená povinnosť informovať by nemala znamenať, že poskytovatelia hostingových služieb majú aktívne vyhľadávať akékoľvek dôkazy o takomto bezprostrednom ohrození života alebo podozrení zo spáchania trestného činu terorizmu. Za dotknutý členský štát by sa mal považovať členský štát, ktorý má právomoc vo veci vyšetrovania a stíhania daných trestných činov terorizmu na základe štátnej príslušnosti páchateľa alebo možnej obete trestného činu alebo cieľového miesta teroristického činu. V prípade pochybností by mali poskytovatelia hostingových služieb predložiť informácie Europolu, ktorý by mal následne postupovať v súlade so svojim mandátom, a to aj tak, že postúpi tieto informácie relevantným vnútroštátnym orgánom. Príslušné orgány členských štátov by mali mať možnosť použiť takéto informácie na prijatie vyšetrovacích opatrení podľa práva Únie alebo vnútroštátneho práva.

([11]) 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).

(42) Poskytovatelia hostingových služieb by mali určiť alebo zriadiť kontaktné miesta, aby uľahčili rýchle vybavovanie príkazov na odstránenie. Kontaktné miesto by malo slúžiť len na operačné účely. Kontaktné miesto by malo pozostávať z akéhokoľvek vyhradeného prostriedku, zabezpečovaného interne alebo externe, ktorý umožní elektronické predkladanie príkazov na odstránenie, a z technických alebo personálnych prostriedkov, ktoré umožnia ich rýchle spracovanie. Nie je potrebné, aby sa kontaktné miesto nachádzalo v Únii. Poskytovateľ hostingových služieb by mal mať možnosť využiť existujúce kontaktné miesto na účely tohto nariadenia pod podmienkou, že toto kontaktné miesto je schopné plniť funkcie stanovené v tomto nariadení. S cieľom zabezpečiť odstránenie teroristického obsahu alebo znemožnenie prístupu k nemu do jednej hodiny od doručenia príkazu na odstránenie by mali byť kontaktné miesta poskytovateľov hostingových služieb vystavených teroristickému obsahu dostupné kedykoľvek. Informácie o kontaktnom mieste by mali zahŕňať informácie o jazyku, v ktorom sa naň možno obrátiť. S cieľom uľahčiť komunikáciu medzi poskytovateľmi hostingových služieb a príslušnými orgánmi sa majú poskytovatelia hostingových služieb nabádať, aby umožnili komunikáciu v niektorom z úradných jazykov inštitúcií Únie, v ktorom sú k dispozícii ich zmluvné podmienky.

(43) Keďže neexistuje všeobecná požiadavka, aby poskytovatelia hostingových služieb zabezpečili fyzickú prítomnosť na území Únie, je potrebné zabezpečiť jednoznačnosť, pokiaľ ide o otázku, do právomoci ktorého členského štátu patrí príslušný poskytovateľ hostingových služieb, ktorý ponúka služby v rámci Únie. Vo všeobecnosti platí, že poskytovateľ hostingových služieb patrí do právomoci toho členského štátu, v ktorom má hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca. Tým by nemali byť dotknuté pravidlá právomoci stanovené na účely príkazov na odstránenie a rozhodnutí prijatých na základe kontroly príkazov na odstránenie podľa tohto nariadenia. Pokiaľ ide o poskytovateľa hostingových služieb, ktorý nemá v Únii žiadne miesto podnikateľskej činnosti a neurčil si právneho zástupcu, každý členský štát by mal mať právomoc a a teda aj možnosť uložiť sankcie pod podmienkou dodržania zásady ne bis in idem.

(44) Tí poskytovatelia hostingových služieb, ktorí nie sú usadení v Únii, by mali písomne určiť právneho zástupcu s cieľom zabezpečiť dodržiavanie a presadzovanie povinností podľa tohto nariadenia. Poskytovatelia hostingových služieb by mali mať možnosť určiť na účely tohto nariadenia právneho zástupcu, ktorý bol už určený na iné účely, ak je tento právny zástupca schopný plniť funkcie stanovené v tomto nariadení. Tento právny zástupca by mal byť splnomocnený konať v mene poskytovateľa hostingových služieb.

(45) Na zabezpečenie účinného vykonávania tohto nariadenia zo strany poskytovateľov hostingových služieb sú potrebné sankcie. Členské štáty by mali prijať pravidlá týkajúce sa sankcií, ktoré môžu mať správnu alebo trestnoprávnu povahu, pričom súčasťou týchto pravidiel môžu byť v relevantných prípadoch aj usmernenia pre ukladanie pokút. Nesplnenie povinnosti v jednotlivých prípadoch by sa mohlo sankcionovať, avšak za súčasného dodržania zásady ne bis in idem a zásady proporcionality, ako aj za súčasného zabezpečenia toho, aby takéto sankcie zohľadňovali systematické zlyhanie. Sankcie by mohli mať rôzne formy vrátane formálnych napomenutí v prípade menej závažných porušení alebo formu peňažných sankcií v súvislosti so závažnejšími alebo systematickejšími porušeniami. Osobitne prísne sankcie by sa mali ukladať, ak poskytovateľ hostingových služieb systematicky neodstraňuje teroristický obsah alebo k nemu systematicky alebo pretrvávajúco neznemožňuje prístup do jednej hodiny od doručenia príkazu na odstránenie. S cieľom zabezpečiť právnu istotu by sa v tomto nariadení malo stanoviť, ktoré porušenia sú sankciované a ktoré okolnosti sú relevantné na posúdenie druhu a úrovne takejto sankcie. Pri určovaní toho, či by sa mali uložiť peňažné sankcie, by sa mali náležite zohľadniť finančné zdroje poskytovateľa hostingových služieb. Príslušný orgán by mal okrem toho zohľadniť, či poskytovateľ hostingových služieb patrí medzi startupy alebo mikropodniky, malé alebo stredné podniky, tak ako je to vymedzené v odporúčaní Komisie 2003/361/ES ([12]). Zohľadniť by sa mali ďalšie okolnosti, ako napríklad to, či bolo konanie poskytovateľa hostingových služieb objektívne neobozretné alebo trestuhodné, alebo či k porušeniu došlo z nedbanlivosti alebo úmyselne. Členské štáty by mali zabezpečiť, aby sankcie uložené za porušenie tohto nariadenia nepodnecovali k odstraňovaniu materiálu, ktorý nie je teroristickým obsahom.

(46) Používanie vzorových formulárov uľahčuje spoluprácu a výmenu informácií medzi príslušnými orgánmi a poskytovateľmi hostingových služieb a umožňuje im rýchlejšie a účinnejšie komunikovať. Je mimoriadne dôležité zabezpečiť rýchlu akciu po doručení príkazu na odstránenie. Vzorové formuláre znižujú náklady na preklad a prispievajú k vyššiemu štandardu postupu. Vzorové formuláre spätnej väzby umožňujú štandardizovanú výmenu informácií, čo je osobitne dôležité v prípadoch, keď poskytovatelia hostingových služieb nie sú schopní splniť príkazy na odstránenie. Autentifikované kanály na predkladanie písomností môžu zaručiť pravosť príkazu na odstránenie vrátane presnosti dátumu a času jeho odoslania a doručenia.

([12]) Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení mikropodnikov, malých a stredných podnikov (Ú. v. EÚ L 124, 20.5.2003, s. 36).

(47) S cieľom umožniť, aby v prípade potreby bolo možné rýchlo zmeniť obsah vzorových 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 k tomuto nariadeniu. S cieľom zohľadniť vývoj v oblasti technológií a súvisiaceho právneho rámca by Komisia mala byť splnomocnená aj na prijímanie delegovaných aktov na doplnenie tohto nariadenia o technické požiadavky na elektronické prostriedky, ktoré majú príslušné orgány používať na zasielanie príkazov na odstránenie. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni expertov, a aby tieto konzultácie vykonávala v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva ([13]). 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 skupín expertov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.

(48) Členské štáty by mali získavať informácie o vykonávaní tohto nariadenia. Členské štáty by mali mať možnosť využiť správy o transparentnosti, ktoré predložili poskytovatelia hostingových služieb, a doplniť ich v prípade potreby podrobnejšími informáciami, ako sú napríklad ich vlastné správy o transparentnosti podľa tohto nariadenia. Na účely hodnotenia vykonávania tohto nariadenia by sa mal vypracovať podrobný program monitorovania výstupov, výsledkov a vplyvov tohto nariadenia.

(49) Komisia by mala vykonať hodnotenie tohto nariadenia do troch rokov odo dňa nadobudnutia jeho účinnosti, a to na základe zistení a záverov v správe o vykonávaní a výsledku monitorovania. Hodnotenie by malo vychádzať z kritérií efektívnosti, nevyhnutnosti, účinnosti, primeranosti, relevantnosti, súdržnosti a pridanej hodnoty Únie. V rámci tohto hodnotenia by sa malo posúdiť fungovanie rôznych operačných a technických opatrení stanovených v tomto nariadení vrátane účinnosti opatrení na posilnenie odhaľovania, identifikácie a odstraňovania teroristického obsahu online, účinnosti mechanizmov záruk, ako aj vplyvov na potenciálne dotknuté základné práva ako je sloboda prejavu a právo na informácie vrátane slobody a plurality médií, slobody podnikania, práva na súkromný život a práva na ochranu osobných údajov. Komisia by mala tiež posúdiť vplyv na potenciálne dotknuté záujmy tretích strán.

(50) Keďže cieľ tohto nariadenia, a to zabezpečenie hladkého fungovania digitálneho jednotného trhu riešením šírenia teroristického obsahu online, nie je možné uspokojivo dosiahnuť na úrovni členských štátov, ale z dôvodov rozsahu a účinkov obmedzenia ho možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o EÚ. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný 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 riešenie zneužívania hostingových služieb na verejné šírenie teroristického obsahu online, najmä o:

a) vhodnej a primeranej povinnosti náležitej starostlivosti, ktoré majú uplatňovať poskytovatelia hostingových služieb s cieľom riešiť verejné šírenie teroristického obsahu prostredníctvom ich služieb a v prípade potreby zabezpečiť jeho rýchle odstránenie alebo znemožnenie prístupu k takémuto obsahu;

([13]) Ú. v. EÚ L 123, 12.5.2016, s. 1.

b) opatreniach, ktoré majú členské štáty zaviesť v súlade s právom Únie a s výhradou vhodných záruk na ochranu základných práv, najmä slobody prejavu a práva na informácie v otvorenej a demokratickej spoločnosti, s cieľom:

i) identifikovať a zabezpečiť rýchle odstránenie teroristického obsahu zo strany poskytovateľov hostingových služieb a

ii) uľahčiť spoluprácu medzi príslušnými orgánmi členských štátov, poskytovateľmi hostingových služieb a v relevantných prípadoch Europolom.

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

3. Materiál verejne šírený na vzdelávacie, novinárske, umelecké alebo výskumné účely alebo na účely predchádzania terorizmu alebo boja proti nemu vrátane materiálu, ktorým sa vyjadrujú polemické alebo kontroverzné názory v rámci verejnej diskusie, sa nepovažuje za teroristický obsah. Vykoná sa posúdenie, ktorým sa určí pravý účel daného šírenia a či sa materiál verejne šíri na uvedené účely.

4. Týmto nariadením sa nemení povinnosť rešpektovať práva, slobody a zásady uvedené v článku 6 Zmluvy o EÚ a jeho uplatňovaním nie sú dotknuté základné zásady slobody prejavu a práva na informácie vrátane slobody a plurality médií.

5. Týmto nariadením nie sú dotknuté smernice 2000/31/ES a 2010/13/EÚ. Pokiaľ ide o audiovizuálne mediálne služby v zmysle článku 1 ods. 1 písm. a) smernice 2010/13/EÚ, prednosť má smernica 2010/13/EÚ.

Článok 2

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje tieto vymedzenia pojmov:

(1) „poskytovateľ hostingových služieb“ je poskytovateľ služieb vymedzených v článku 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535 ([14]), ktoré pozostávajú z uchovávania informácií poskytnutých poskytovateľom obsahu a na jeho žiadosť;

(2) „poskytovateľ obsahu“ je používateľ, ktorý poskytol informácie, ktoré uchováva alebo uchoval a verejne šíri poskytovateľ hostingových služieb;

(3) „verejné šírenie “ je sprístupnenie informácií na žiadosť poskytovateľa obsahu potenciálne neobmedzenému počtu osôb;

(4) „ponúkať služby v Únii“ je umožňovať fyzickým alebo právnickým 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;

(5) „podstatná väzba“ je väzba poskytovateľa hostingových služieb na jeden alebo viacero členských štátov, ktorá je z dôvodu miesta jeho podnikateľskej činnosti v Únii alebo z dôvodu konkrétnych skutkových kritérií, ako sú:

a) existencia značného počtu používateľov jeho služieb v jednom alebo vo viacerých členských štátoch; alebo

b) zameranie jeho činností na jeden alebo viacero členských štátov;

(6) „trestné činy terorizmu“ sú trestné činy vymedzené v článku 3 smernice (EÚ) 2017/541;

([14]) Smernica Európskeho parlamentu a Rady (EÚ) 2015/1535 z 9. septembra 2015, ktorou sa stanovuje postup pri poskytovaní informácií v oblasti technických predpisov a pravidiel vzťahujúcich sa na služby informačnej spoločnosti (Ú. v. EÚ L 241, 17.9.2015, s. 1).

(7) „teroristický obsah“ je jeden alebo viacero z týchto druhov materiálov, a to materiálu, ktorý:

a) podnecuje na spáchanie niektorého z trestných činov uvedených v článku 3 ods. 1 písm. a) až i) smernice (EÚ) 2017/541, ak takýto materiál, či už priamo alebo nepriamo, napríklad glorifikáciou teroristických činov, obhajuje páchanie trestných činov terorizmu, a tým spôsobuje nebezpečenstvo spáchania jedného alebo viacerých takýchto trestných činov;

b) navádza osobu alebo skupiny osôb na spáchanie alebo podporu spáchania niektorého z trestných činov uvedených v článku 3 ods. 1 písm. a) až i) smernice (EÚ) 2017/541;

c) navádza osobu alebo skupiny osôb na účasť na činnostiach teroristickej skupiny v zmysle článku 4 písm. b) smernice (EÚ) 2017/541;

d) poskytuje návod na výrobu alebo použitie výbušnín, strelných zbraní alebo iných zbraní, alebo škodlivých alebo nebezpečných látok, alebo iných osobitných metód alebo techník na účely spáchania alebo podpory spáchania niektorého z trestných činov terorizmu uvedených v článku 3 ods. 1 písm. a) až i) smernice (EÚ) 2017/541;

e) vytvára hrozbu spáchania niektorého z trestných činov uvedených v článku 3 ods. 1 písm. a) až i) smernice (EÚ) 2017/541;

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

(9) „hlavné miesto podnikateľskej činnosti“ je ústredie alebo sídlo poskytovateľa hostingovej služby, kde sa vykonávajú hlavné finančné operácie a prevádzková kontrola.

ODDIEL II

OPATRENIA NA RIEŠENIE ŠÍRENIA TERORISTICKÉHO OBSAHU ONLINE

Článok 3

Príkazy na odstránenie

1. Príslušný orgán každého členského štátu má právomoc vydať príkaz na odstránenie, ktorým sa poskytovateľom hostingových služieb ukladá povinnosť odstrániť teroristický obsah alebo znemožniť prístup k teroristickému obsahu vo všetkých členských štátoch.

2. Ak príslušný orgán predtým nevydal voči poskytovateľovi hostingových služieb príkaz na odstránenie, informuje poskytovateľa hostingových služieb o uplatniteľných postupoch a lehotách najmenej 12 hodín pred vydaním príkazu na odstránenie.

Prvý pododsek sa neuplatňuje v riadne odôvodnených naliehavých prípadoch.

3. Poskytovatelia hostingových služieb odstránia teroristický obsah alebo znemožnia prístup k teroristickému obsahu vo všetkých členských štátoch čo najskôr, najneskôr však do jednej hodiny od doručenia príkazu na odstránenie.

4. Príslušné orgány vydajú príkazy na odstránenie použitím vzorového formuláru uvedeného v prílohe I. Príkazy na odstránenie obsahujú tieto prvky:

a) identifikačné údaje príslušného orgánu, ktorý vydal príkaz na odstránenie, a autentifikáciu príkazu na odstránenie daným príslušným orgánom;

b) dostatočne podrobné odôvodnenie, v ktorom sa vysvetľuje, prečo sa obsah považuje za teroristický obsah, a odkaz na príslušné druhy materiálu uvedené v článku 2 bode 7;

c) presnú jednotnú adresu zdroja (URL) a v prípade potreby aj ďalšie informácie umožňujúce identifikáciu teroristického obsahu;

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

e) dátum, odtlačok pečiatky s časom vydania a elektronický podpis príslušného orgánu vydávajúceho príkaz na odstránenie;

f) ľahko zrozumiteľné informácie o prostriedkoch nápravy, ktoré majú poskytovateľ hostingových služieb a poskytovateľ obsahu k dispozícii, vrátane informácií o prostriedku nápravy, ktorý možno podať na príslušný orgán, a o možnosti obrátiť sa na súd, ako aj lehoty na podanie opravných prostriedkov;

g) ak je to potrebné a primerané, rozhodnutie o nezverejnení informácií o odstránení teroristického obsahu alebo o znemožnení prístupu k nemu v súlade s článkom 11 ods. 3

5. Príslušný orgán adresuje príkaz na odstránenie hlavnému miestu podnikateľskej činnosti poskytovateľa hostingových služieb alebo jeho právnemu zástupcovi určenému v súlade s článkom 17.

Príslušný orgán zašle príkaz na odstránenie kontaktnému miestu uvedenému v článku 15 ods. 1 elektronickými prostriedkami, ktoré umožňujú vyhotovenie písomného záznamu za podmienok umožňujúcich autentifikáciu odosielateľa, ako aj stanovenie presného dátumu a času odoslania a doručenia príkazu.

6. Poskytovateľ hostingových služieb bez zbytočného odkladu informuje príslušný orgán prostredníctvom vzorového formulára uvedeného v prílohe II o odstránení teroristického obsahu alebo o znemožnení prístupu k teroristickému obsahu vo všetkých členských štátoch, pričom uvedie najmä čas tohto odstránenia alebo znemožnenia prístupu.

7. Ak poskytovateľ hostingových služieb nemôže splniť príkaz na odstránenie z dôvodu vyššej moci alebo faktickej nemožnosti vykonať ho, ktorú nezavinil poskytovateľ hostingových služieb, vrátane objektívne odôvodniteľných technických alebo operačných príčin, bez zbytočného odkladu informuje o týchto dôvodoch príslušný orgán, ktorý vydal tento príkaz na odstránenie, a to prostredníctvom vzorového formulára uvedeného v prílohe III.

Lehota uvedená v odseku 3 začne plynúť, hneď ako pominú dôvody uvedené v prvom pododseku tohto odseku.

8. Ak poskytovateľ hostingových služieb nemôže splniť príkaz na odstránenie, pretože obsahuje zjavné chyby alebo neobsahuje dostatočné informácie na jeho vykonanie, bez zbytočného odkladu informuje príslušný orgán, ktorý vydal tento príkaz na odstránenie, a požiada ho o potrebné objasnenie, pričom použije vzorový formulár uvedený v prílohe III.

Lehota uvedená v odseku 3 začne plynúť hneď, ako poskytovateľ hostingových služieb dostane potrebné objasnenie.

9. Príkaz na odstránenie sa stane konečným po márnom uplynutí lehoty na podanie opravného prostriedku podľa vnútroštátneho práva alebo po potvrdení rozhodnutia v konaní o opravnom prostriedku.

Po tom, ako sa príkaz na odstránenie stane konečným, príslušný orgán, ktorý ho vydal, o tom informuje príslušný orgán uvedený v článku 12 ods. 1 písm. c) členského štátu, v ktorom má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca.

Článok 4

Postup pre cezhraničné príkazy na odstránenie

1. S výhradou článku 3, ak poskytovateľ hostingových služieb nemá svoje hlavné miesto podnikateľskej činnosti ani právneho zástupcu v členskom štáte príslušného orgánu, ktorý vydal príkaz na odstránenie, daný orgán súčasne predloží kópiu príkazu na odstránenie príslušnému orgánu členského štátu, v ktorom má poskytovateľ hostingových služieb svoje hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca.

2. Ak sa poskytovateľovi hostingových služieb doručí príkaz na odstránenie, ako sa uvádza v tomto článku, prijme opatrenia stanovené v článku 3 a potrebné opatrenia, ktoré mu umožnia obnoviť obsah alebo opätovne umožniť prístup k nemu podľa odseku 7 tohto článku.

3. Príslušný orgán členského štátu, v ktorom má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca, môže z vlastného podnetu do 72 hodín od doručenia kópie príkazu na odstránenie v súlade s odsekom 1 skontrolovať príkaz na odstránenie s cieľom zistiť, či závažným alebo zjavným spôsobom neporušuje toto nariadenie alebo základné práva a slobody, ktoré zaručuje charta.

Ak zistí porušenie, v rovnakej lehote prijme o tomto zistení odôvodnené rozhodnutie.

4. Poskytovatelia hostingových služieb a poskytovatelia obsahu sú oprávnení predložiť do 48 hodín od doručenia príkazu na odstránenie alebo informácií podľa článku 11 ods. 2 odôvodnenú žiadosť príslušnému orgánu členského štátu, v ktorom má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca, aby skontroloval príkaz na odstránenie podľa odseku 3 prvého pododseku tohto článku.

Tento príslušný orgán do 72 hodín od doručenia žiadosti prijme po skontrolovaní príkazu na odstránenie odôvodnené rozhodnutie, v ktorom uvedie svoje zistenie, či došlo k porušeniu.

5. Príslušný orgán pred prijatím rozhodnutia podľa odseku 3 druhého pododseku alebo rozhodnutia o zistení porušenia podľa odseku 4 druhého pododseku informuje príslušný orgán, ktorý vydal príkaz na odstránenie, o svojom zámere prijať rozhodnutie a o dôvodoch jeho prijatia.

6. Ak príslušný orgán členského štátu, v ktorom má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca, prijme odôvodnené rozhodnutie v súlade s odsekom 3 alebo 4 tohto článku, toto rozhodnutie bezodkladne oznámi príslušnému orgánu, ktorý vydal príkaz na odstránenie, poskytovateľovi hostingových služieb, poskytovateľovi obsahu, ktorý požiadal o kontrolu podľa odseku 4 tohto článku, a v súlade s článkom 14 aj Europolu. Ak sa v rozhodnutí zistí porušenie podľa odseku 3 alebo 4 tohto článku, právne účinky príkazu na odstránenie zaniknú.

7. Po doručení rozhodnutia o zistení porušenia oznámeného v súlade s odsekom 6 okamžite obnoví dotknutý poskytovateľ hostingových služieb obsah alebo umožní prístup k nemu, bez toho, aby bola dotknutá jeho možnosť uplatniť svoje zmluvné podmienky v súlade s právom Únie a vnútroštátnym právom.

Článok 5

Osobitné opatrenia

(1) Poskytovateľ hostingových služieb vystavený teroristickému obsahu, ako sa uvádza v odseku 4, v relevantných prípadoch zahrnie do svojich zmluvných podmienok a uplatňuje ustanovenia na riešenie zneužívania svojich služieb na verejné šírenie teroristického obsahu.

Postupuje pri tom dôsledne, primerane a nediskriminačne, pričom za každých okolností náležite zohľadňuje základné práva používateľov a berie ohľad najmä na zásadný význam slobody prejavu a práva na informácie v otvorenej a demokratickej spoločnosti s cieľom zabrániť odstráneniu obsahu, ktorý nie je teroristickým obsahom.

2. Poskytovateľ hostingových služieb vystavený teroristickému obsahu, ako sa uvádza v odseku 4, prijme osobitné opatrenia na ochranu svojich služieb pred verejným šírením teroristického obsahu.

Rozhodnutie o výbere osobitných opatrení prináleží poskytovateľovi hostingových služieb. Takéto opatrenia môžu zahŕňať jedno alebo viacero z týchto opatrení:

a) primerané technické a operačné opatrenia alebo kapacity, ako napríklad primerané personálne zabezpečenie alebo technické prostriedky na identifikáciu a rýchle odstránenie teroristického obsahu alebo znemožnenie prístupu k nemu;

b) ľahko dostupné a používateľsky ústretové mechanizmy, prostredníctvom ktorých môžu používatelia poskytovateľovi hostingových služieb nahlasovať alebo označovať potenciálny teroristický obsah;

c) akékoľvek iné mechanizmy na zvýšenie informovanosti o teroristickom obsahu v rámci jeho služieb, ako sú mechanizmy používateľského moderovania.

d) akékoľvek iné opatrenie, ktoré poskytovateľ hostingových služieb považuje za vhodné na riešenie dostupnosti teroristického obsahu v rámci svojich služieb.

3. Osobitné opatrenia musia spĺňať všetky tieto požiadavky:

a) sú účinné pri zmierňovaní úrovne vystavenia služieb poskytovateľa hostingových služieb teroristickému obsahu;

b) sú cielené a primerané, pričom zohľadňujú najmä závažnosť úrovne vystavenia služieb poskytovateľa hostingových služieb teroristickému obsahu, ako aj technické a operačné spôsobilosti, finančnú silu, počet používateľov služieb poskytovateľa hostingových služieb a množstvo obsahu, ktorý poskytujú;

c) pri ich uplatňovaní sa plne zohľadňujú práva a oprávnené záujmy používateľov, najmä ich základné práva, ktorými sú sloboda prejavu a právo na informácie, rešpektovanie súkromného života a ochrana osobných údajov;

d) uplatňujú sa dôsledne a nediskriminačne.

Ak osobitné opatrenia zahŕňajú použitie technických opatrení, poskytnú sa primerané a účinné záruky, najmä prostredníctvom ľudského dohľadu a overovania, s cieľom zabezpečiť správnosť a zabrániť odstráneniu materiálu, ktorý nie je teroristickým obsahom.

4. Poskytovateľ hostingových služieb je vystavený teroristickému obsahu, ak príslušný orgán členského štátu, v ktorom má hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca:

a) prijal rozhodnutie založené na objektívnych faktoroch, ako je napríklad skutočnosť, že za uplynulých 12 mesiacov boli poskytovateľovi hostingových služieb doručené dva alebo viac konečných príkazov na odstránenie, o zistení, že poskytovateľ hostingových služieb je vystavený teroristickému obsahu; a

b) oznámil rozhodnutie uvedené v písmene a) poskytovateľovi hostingových služieb.

5. Po doručení rozhodnutia uvedeného v odseku 4 alebo v relevantných prípadoch v odseku 6 poskytovateľ hostingových služieb nahlási príslušnému orgánu osobitné opatrenia, ktoré prijal a ktoré zamýšľa prijať v záujme splnenia odsekov 2 a 3. Urobí tak do troch mesiacov od doručenia rozhodnutia a potom raz ročne. Táto povinnosť zanikne, keď príslušný orgán rozhodne na základe žiadosti podľa odseku 7, že daný poskytovateľ hostingových služieb už nie je vystavený teroristickému obsahu.

6. Ak sa príslušný orgán na základe hlásení uvedených v odseku 5 a prípadne akýchkoľvek iných objektívnych faktorov domnieva, že prijaté osobitné opatrenia nespĺňajú odseky 2 a 3, zašle poskytovateľovi hostingových služieb rozhodnutie, v ktorom mu uloží povinnosť prijať opatrenia potrebné na zabezpečenie splnenia odsekov 2 a 3.

Poskytovateľ hostingových služieb si môže vybrať, ktorý typ osobitných opatrení prijme.

7. Poskytovateľ hostingových služieb môže kedykoľvek požiadať príslušný orgán o preskúmanie a prípadnú zmenu alebo zrušenie rozhodnutia uvedeného v odseku 4 alebo 6.

Príslušný orgán do troch mesiacov od doručenia žiadosti prijme o tejto žiadosti odôvodnené rozhodnutie založené na objektívnych faktoroch a informuje o ňom poskytovateľa hostingových služieb.

8. Žiadnou požiadavkou prijať osobitné opatrenia nie je dotknutý článok 15 ods. 1 smernice 2000/31/ES a nevyplýva z nej všeobecná povinnosť poskytovateľov hostingových služieb monitorovať informácie, ktoré prenášajú alebo uchovávajú, ani všeobecná povinnosť aktívne zisťovať skutočnosti alebo okolnosti, ktoré naznačujú protiprávne konanie.

Žiadnou požiadavkou prijať osobitné opatrenia sa poskytovateľovi hostingových služieb nesmie ukladať povinnosť používať automatizované nástroje.

Článok 6

Uchovávanie obsahu a súvisiacich údajov

1. Poskytovatelia hostingových služieb uchovávajú teroristický obsah, ktorý bol odstránený alebo ku ktorému bol znemožnený prístup v dôsledku príkazu na odstránenie alebo osobitných opatrení podľa článkov 3 alebo 5, ako aj súvisiace údaje odstránené v dôsledku odstránenia takéhoto teroristického obsahu, ktoré sú potrebné na:

a) správne alebo súdne preskúmanie alebo vybavovanie sťažností podľa článku 10 v súvislosti s rozhodnutím o odstránení teroristického obsahu a súvisiacich údajov alebo znemožnení prístupu k nim; alebo

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

2. Teroristický obsah a súvisiace údaje uvedené v odseku 1 sa uchovávajú šesť mesiacov od odstránenia alebo znemožnenia prístupu k nim. Teroristický obsah sa na žiadosť príslušného orgánu alebo súdu uchováva počas ďalšieho stanoveného obdobia iba vtedy, ak je to potrebné na účely prebiehajúceho správneho alebo súdneho preskúmania podľa odseku 1 písm. a), a len na čas potrebný pre uvedené konania.

3. Poskytovatelia hostingových služieb zabezpečia, aby sa na teroristický obsah a súvisiace údaje uchovávané podľa odseku 1 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 7

Povinnosti poskytovateľov hostingových služieb týkajúce sa transparentnosti

1. Poskytovatelia hostingových služieb vo svojich zmluvných podmienkach jasne stanovia svoju politiku riešenia šírenia teroristického obsahu vrátane prípadného relevantného vysvetlenia fungovania osobitných opatrení, čo v relevantných prípadoch zahŕňa aj používanie automatizovaných nástrojov.

2. Poskytovateľ hostingových služieb, ktorý v určitom kalendárnom roku podnikol kroky proti šíreniu teroristického obsahu alebo ktorému sa uložila povinnosť podniknúť takéto kroky podľa tohto nariadenia, zverejní správu o transparentnosti týkajúcu sa týchto krokov v danom roku. Túto správu uverejní do 1. marca nasledujúceho roka.

3. Správy o transparentnosti obsahujú aspoň tieto informácie:

a) informácie o opatreniach poskytovateľa hostingových služieb v súvislosti s identifikáciou a odstraňovaním teroristického obsahu alebo znemožnením prístupu k nemu;

b) informácie o opatreniach poskytovateľa hostingových služieb na účely riešenia opätovného výskytu materiálu online, ktorý bol predtým odstránený alebo ku ktorému bol znemožnený prístup, pretože sa považoval za teroristický obsah, najmä ak sa použili automatizované nástroje;

c) počet položiek teroristického obsahu, ktorý bol odstránený alebo ku ktorému bol znemožnený prístup na základe príkazov na odstránenie alebo osobitných opatrení, a počet príkazov na odstránenie, v prípade ktorých obsah nebol odstránený alebo k nemu nebol znemožnený prístup podľa článku 3 ods. 7 prvého pododseku a článku 3 ods. 8 prvého pododseku, spolu s dôvodmi neodstránenia alebo neznemožnenia prístupu;

d) počet a výsledky sťažností, ktoré vybavil poskytovateľ hostingových služieb v súlade s článkom 10;

e) počet a výsledky správnych alebo súdnych preskúmaní začatých poskytovateľom hostingových služieb;

f) počet prípadov, v ktorých bol poskytovateľ hostingových služieb v dôsledku správneho alebo súdneho preskúmania povinný obnoviť obsah alebo prístup k nemu;

g) počet prípadov, v ktorých poskytovateľ hostingových služieb obnovil obsah alebo prístup k nemu po sťažnosti zo strany poskytovateľa obsahu.

Článok 8

Správy o transparentnosti príslušných orgánov

1. Príslušné orgány uverejňujú výročné správy o transparentnosti týkajúce sa ich činností podľa tohto nariadenia. Tieto správy obsahujú v súvislosti s daným kalendárnym rokom aspoň tieto informácie:

a) počet príkazov na odstránenie vydaných podľa článku 3 upresňujúcich počet príkazov na odstránenie podliehajúcich článku 4 ods. 1, počet príkazov na odstránenie skontrolovaných podľa článku 4 a informácie o vykonaní týchto príkazov na odstránenie dotknutými poskytovateľmi hostingových služieb, vrátane počtu prípadov, v ktorých teroristický obsah bol odstránený alebo bol znemožnený prístup k nemu a počtu prípadov, v ktorých teroristický obsah nebol odstránený ani k nemu nebol znemožnený prístup;

b) počet rozhodnutí prijatých podľa článku 5 ods. 4, 6 alebo 7 a informácie o vykonaní týchto rozhodnutí poskytovateľmi hostingových služieb, vrátane opisu osobitných opatrení;

c) počet prípadov, v ktorých boli príkazy na odstránenie a rozhodnutia prijaté v súlade s článkom 5 ods. 4 a 6 predmetom správneho alebo súdneho preskúmania, a informácie o výsledku príslušných konaní;

d) počet rozhodnutí, ktorými sa ukladajú sankcie podľa článku 18 a opis druhu uloženej sankcie.

2. Výročné správy o transparentnosti uvedené v odseku 1 nesmú obsahovať informácie, ktoré môžu mať vplyv na prebiehajúce činnosti zamerané na predchádzanie trestným činom terorizmu alebo ich odhaľovanie, vyšetrovanie či stíhanie alebo na záujmy národnej bezpečnosti.

Článok 9

Prostriedky nápravy

1. Poskytovatelia hostingových služieb, ktorým bol doručený príkaz na odstránenie vydaný podľa článku 3 ods. 1 alebo rozhodnutie podľa článku 4 ods. 4 alebo podľa článku 5 ods. 4, 6 alebo 7, majú právo na účinný prostriedok nápravy. Toto právo zahŕňa právo napadnúť takýto príkaz na odstránenie na súdoch členského štátu príslušného orgánu, ktorý vydal daný príkaz na odstránenie a právo napadnúť takéto rozhodnutie podľa článku 4 ods. 4 alebo podľa článku 5 ods. 4, 6 alebo 7 na súdoch členského štátu príslušného orgánu, ktorý prijal dané rozhodnutie.

2. Poskytovatelia obsahu, ktorých obsah bol odstránený alebo ku ktorému bol znemožnený prístup v dôsledku príkazu na odstránenie, majú právo na účinný prostriedok nápravy. Toto právo zahŕňa právo napadnúť príkaz na odstránenie vydaný podľa článku 3 ods. 1 na súdoch členského štátu príslušného orgánu, ktorý vydal príkaz na odstránenie a právo napadnúť rozhodnutie podľa článku 4 ods. 4 na súdoch členského štátu príslušného orgánu, ktorý prijal dané rozhodnutie.

3. Členské štáty zavedú účinné postupy na uplatňovanie práv uvedených v tomto článku.

Článok 10

Mechanizmy podávania sťažností

1. Každý poskytovateľ hostingových služieb zavedie účinný a prístupný mechanizmus umožňujúci poskytovateľom obsahu, ak ich obsah bol odstránený alebo bol k nemu znemožnený prístup v dôsledku osobitných opatrení podľa článku 5, podať sťažnosť voči odstráneniu obsahu alebo znemožneniu prístupu k nemu, v ktorej požiadajú o obnovenie obsahu alebo prístupu k nemu.

2. Každý poskytovateľ hostingových služieb bezodkladne preskúma všetky sťažnosti doručené prostredníctvom mechanizmu uvedeného v odseku 1 a bez zbytočného odkladu obnoví obsah alebo prístup k nemu, ak bolo jeho odstránenie alebo znemožnenie prístupu k nemu neopodstatnené. O výsledku preskúmania informuje sťažovateľa do dvoch týždňov od doručenia sťažnosti.

Ak je sťažnosť zamietnutá, poskytovateľ hostingových služieb uvedie sťažovateľovi dôvody svojho rozhodnutia.

Obnovenie obsahu alebo prístupu k nemu nebráni správnemu alebo súdnemu preskúmaniu napádajúcemu rozhodnutie poskytovateľa hostingových služieb alebo príslušného orgánu.

Článok 11

Informácie pre poskytovateľov obsahu

1. Ak poskytovateľ hostingových služieb odstráni teroristický obsah alebo k nemu znemožní prístup, sprístupní poskytovateľovi obsahu informácie o takomto odstránení alebo o znemožnení prístupu.

2. Na žiadosť poskytovateľa obsahu poskytovateľ hostingových služieb buď informuje poskytovateľa obsahu o dôvodoch odstránenia alebo znemožnenia prístupu a o jeho právach napadnúť príkaz na odstránenie alebo poskytne poskytovateľovi obsahu kópiu príkazu na odstránenie.

3. Povinnosť podľa odsekov 1 a 2 sa neuplatňuje, ak príslušný orgán, ktorý vydal príkaz na odstránenie, rozhodne, že je nevyhnutné a primerané, aby dôvodov verejnej bezpečnosti, ako je napríklad predchádzanie trestným činom terorizmu, ich vyšetrovanie, odhaľovanie a stíhanie, nedošlo k zverejneniu, a to tak dlho, ako je to potrebné, nie však viac ako šesť týždňov od príslušného rozhodnutia. V takom prípade poskytovateľ hostingových služieb nezverejní žiadne informácie o odstránení teroristického obsahu alebo o znemožnení prístupu k nemu.

Uvedený príslušný orgán môže predĺžiť túto lehotu o ďalších šesť týždňov, ak je takéto nezverejnenie naďalej opodstatnené.

ODDIEL IV

PRÍSLUŠNÉ ORGÁNY A SPOLUPRÁCA

Článok 12

Určenie príslušných orgánov

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

a) vydávanie príkazov na odstránenie podľa článku 3;

b) kontrolu príkazov na odstránenie podľa článku 4;

c) dohľad nad vykonávaním osobitných opatrení podľa článku 5;

d) uloženie sankcií podľa článku 18.

2. Každý členský štát zabezpečí, aby sa určilo alebo zriadilo kontaktné miesto v rámci príslušného orgánu uvedeného v odseku 1 písm. a) na vybavovanie žiadostí o objasnenie a spätnú väzbu v súvislosti s príkazmi na odstránenie, ktoré daný príslušný orgán vydal.

Členské štáty zabezpečia, aby sa informácie o kontaktnom mieste sprístupnili verejnosti.

3. Členské štáty oznámia Komisii príslušný orgán alebo orgány uvedené v odseku 1 a všetky ich zmeny do 7. júna 2022. Komisia uverejní oznámenie a všetky jeho zmeny v *Úradnom vestníku Európskej únie*.

4. Do 7. júna 2022 zriadi Komisia online register so zoznamom príslušných orgánov uvedených v odseku 1 a kontaktných miest jednotlivých príslušných orgánov určených alebo zriadených podľa odseku 2. Komisia pravidelne uverejňuje všetky jeho zmeny.

Článok 13

Príslušné orgány

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

2. Členské štáty zabezpečia, aby ich príslušné orgány pri plnení svojich úloh podľa tohto nariadenia konali objektívne a nediskriminačne a plne dodržiavali základné práva. Príslušné orgány nežiadajú ani neprijímajú pokyny od žiadneho iného orgánu v súvislosti s plnením svojich úloh podľa článku 12 ods. 1

Prvým pododsekom nie je dotknutý dohľad v súlade s vnútroštátnym ústavným právom.

Článok 14

Spolupráca medzi poskytovateľmi hostingových služieb, príslušnými orgánmi a Europolom

1. Príslušné orgány sa v súvislosti s príkazmi na odstránenie navzájom informujú, koordinujú svoju činnosť a spolupracujú a vo vhodných prípadoch do týchto aktivít zapájajú Europol, najmä aby sa predišlo duplicite úsilia, posilnila sa koordinácia a aby sa predišlo zásahom do vyšetrovaní v rôznych členských štátoch.

2. Príslušné orgány v členských štátoch sa navzájom informujú s príslušnými orgánmi uvedenými v článku 12 ods. 1 písm. c) a d), koordinujú s nimi svoju činnosť a spolupracujú s nimi, pokiaľ ide o osobitné opatrenia prijaté podľa článku 5 a sankcie uložené podľa článku 18. Členské štáty zabezpečia, aby mali príslušné orgány uvedené v článku 12 ods. 1 písm. c) a d) všetky príslušné informácie.

3. Na účely odseku 1 členské štáty poskytnú vhodné a zabezpečené komunikačné kanály alebo mechanizmy, ktorými sa zaistí, aby sa príslušné informácie vymieňali včas.

4. V záujme účinného vykonávania tohto nariadenia, ako aj zabránenia duplicite úsilia môžu členské štáty a poskytovatelia hostingových služieb využiť špecializované nástroje vrátane nástrojov vytvorených Europolom s cieľom uľahčiť najmä:

a) spracovanie a spätnú väzbu v súvislosti s príkazmi na odstránenie podľa článku 3; a

b) spoluprácu s cieľom identifikovať a vykonávať osobitné opatrenia podľa článku 5.

5. Ak sa poskytovatelia hostingových služieb dozvedia o teroristickom obsahu, ktorý zahŕňa bezprostredné ohrozenie života, bezodkladne informujú orgány príslušné na vyšetrovanie a stíhanie trestných činov v dotknutých členských štátoch. Ak nie je možné identifikovať dotknuté členské štáty, poskytovatelia hostingových služieb informujú kontaktné miesto podľa článku 12 ods. 2 v členskom štáte, v ktorom majú hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený ich právny zástupca, pričom informácie o teroristickom obsahu zašlú aj Europolu, aby podnikol vhodné nadväzujúce kroky.

6. Príslušné orgány sa nabádajú, aby zasielali kópie príkazov na odstránenie Europolu, čím mu umožnia vypracovať výročnú správu, ktorá bude zahŕňať analýzy druhov teroristického obsahu, na ktoré sa vzťahujú príkazy na odstránenie alebo znemožnenie prístupu k nemu podľa tohto nariadenia.

Článok 15

Kontaktné miesta poskytovateľov hostingových služieb

1. Poskytovateľ hostingových služieb určí alebo zriadi kontaktné miesto na doručovanie príkazov na odstránenie elektronickými prostriedkami a na ich rýchle vybavenie podľa článkov 3 a 4. Poskytovateľ hostingových služieb zabezpečí, aby boli informácie o kontaktnom mieste verejne prístupné.

2. V informáciách podľa odseku 1 tohto článku sa uvedú úradné jazyky inštitúcií Únie uvedené v nariadení č. 1/58 ([15]), v ktorých sa možno na kontaktné miesto obrátiť a v ktorých sa má uskutočniť ďalšia komunikácia v súvislosti s príkazmi na odstránenie podľa článku 3. Medzi tieto jazyky patrí aspoň jeden z úradných jazykov členského štátu, v ktorom má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca.

ODDIEL V

VYKONÁVANIE A PRESADZOVANIE

Článok 16

Právomoc

1. Právomoc na účely článkov 5, 18 a 21 má členský štát, v ktorom sa nachádza hlavné miesto podnikateľskej činnosti poskytovateľa hostingových služieb. Poskytovateľ hostingových služieb, ktorý nemá hlavné miesto podnikateľskej činnosti v Únii, sa považuje za poskytovateľa v právomoci členského štátu, v ktorom má pobyt alebo je usadený jeho právny zástupca.

2. Ak poskytovateľ hostingových služieb, ktorého hlavné miesto podnikateľskej činnosti sa nenachádza v Únii, neurčí právneho zástupcu, majú právomoc všetky členské štáty.

3. Ak sa príslušný orgán členského štátu vykonáva právomoc podľa odseku 2, informuje o tom príslušné orgány všetkých ostatných členských štátov.

Článok 17

Právny zástupca

1. Poskytovateľ hostingových služieb, ktorý nemá hlavné miesto podnikateľskej činnosti v Únii, písomne určí fyzickú alebo právnickú osobu za svojho právneho zástupcu v Únii na účely doručovania, výkonu a presadzovania príkazov na odstránenie a rozhodnutí vydaných príslušnými orgánmi.

2. Poskytovateľ hostingových služieb udelí svojmu právnemu zástupcovi potrebné právomoci a zdroje, aby mohol vykonávať dané príkazy na odstránenie a rozhodnutia a spolupracovať s príslušnými orgánmi.

Právny zástupca musí mať pobyt alebo byť usadený v jednom z členských štátov, v ktorých poskytovateľ hostingových služieb ponúka svoje služby.

3. Právny zástupca môže niesť zodpovednosť za porušenie tohto nariadenia bez toho, aby bola dotknutá zodpovednosť alebo právne kroky voči poskytovateľovi hostingových služieb.

4. Poskytovateľ hostingových služieb oznámi určenie svojho právneho zástupcu príslušnému orgánu uvedenému v článku 12 ods. 1 písm. d) v členskom štáte, v ktorom má pobyt alebo je usadený tento právny zástupca.

Poskytovateľ hostingových služieb sprístupní informácie o právnom zástupcovi verejnosti.

ODDIEL VI

ZÁVEREČNÉ USTANOVENIA

Článok 18

Sankcie

1. Členské štáty stanovia pravidlá o sankciách uplatniteľných za porušenie tohto nariadenia poskytovateľom hostingových služieb a prijmú všetky nevyhnutné opatrenia na zabezpečenie ich vykonávania. Takéto sankcie sa obmedzia na porušenie povinností podľa článku 3 ods. 3 a 6, článku 4 ods. 2 a 7, článku 5 ods. 1, 2, 3, 5 a 6, článkov 6, 7, 10 a 11, článku 14 ods. 5, článku 15 ods. 1 a článku 17.

([15]) Nariadenie č. 1 o používaní jazykov v Európskom hospodárskom spoločenstve (Ú. v. ES 17, 6.10.1958, s. 385).

Sankcie uvedené v prvom pododseku musia byť účinné, primerané a odrádzajúce. Členské štáty do 7. júna 2022 oznámia tieto pravidlá a opatrenia Komisii a bezodkladne jej oznámia všetky následné zmeny, ktoré sa ich týkajú.

2. Členské štáty zabezpečia, aby príslušné orgány pri rozhodovaní o tom, či uložia sankciu, a pri určovaní druhu a sadzby sankcie zohľadnili všetky relevantné okolnosti vrátane:

a) povahy, závažnosti a dĺžky trvania porušenia;

b) toho, či išlo úmyselné porušenie alebo porušenie z nedbanlivosti;

c) predchádzajúcich porušení, ktorých sa dopustil poskytovateľ hostingových služieb;

d) finančnej sily poskytovateľa hostingových služieb;

e) miery spolupráce poskytovateľa hostingových služieb s príslušnými orgánmi;

f) povahy a veľkosti poskytovateľa hostingových služieb, najmä či ide o mikropodnik, malý alebo stredný podnik;

g) miery zavinenia zo strany poskytovateľa hostingových služieb, pričom sa zohľadnia technické a organizačné opatrenia, ktoré poskytovateľ hostingových služieb prijal na účely splnenia tohto nariadenia.

3. Členské štáty zabezpečia, aby systematické alebo pretrvávajúce neplnenie povinností podľa článku 3 ods. 3 podliehalo peňažným sankciám až do výšky 4 % celosvetového obratu poskytovateľa hostingových služieb za predchádzajúci finančný rok.

Článok 19

Technické požiadavky a zmeny príloh

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

2. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 20 s cieľom zmeniť prílohy s cieľom účinne riešiť prípadnú potrebu zlepšenia v súvislosti s obsahom vzorových formulárov príkazov na odstránenie a poskytnúť informácie o nemožnosti vykonať príkazy na odstránenie.

Článok 20

Vykonávanie delegovania právomoci

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

2. Právomoc prijímať delegované akty uvedené v článku 19 sa Komisii udeľuje na dobu neurčitú od 7. júna 2022.

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

4. Komisia pred prijatím delegovaného aktu konzultuje s expertmi určenými jednotlivými členskými štátmi v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva.

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

6. Delegovaný 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 získavajú od svojich príslušných orgánov a poskytovateľov hostingových služieb, ktorí patria do ich právomoci, informácie o krokoch, ktoré podnikli v súlade s týmto nariadením počas predošlého kalendárneho roka, a každý rok do 31. marca ich zašlú Komisii. Tieto informácie zahŕňajú:

a) počet vydaných príkazov na odstránenie a počet položiek teroristického obsahu, ktorý bol odstránený alebo ku ktorému bol znemožnený prístup, a rýchlosť odstránenia alebo znemožnenia prístupu;

b) osobitné opatrenia prijaté podľa článku 5 vrátane počtu položiek teroristického obsahu, ktorý bol odstránený alebo ku ktorému bol znemožnený prístup, a rýchlosť odstránenia alebo znemožnenia prístupu;

c) počet žiadostí o prístup vydaných príslušnými orgánmi, pokiaľ ide o obsah uchovávaný poskytovateľmi hostingových služieb podľa článku 6;

d) počet začatých konaní vo veci sťažnosti a krokov zo strany poskytovateľov hostingových služieb podľa článku 10;

e) počet začatých správnych alebo súdnych preskúmaní a rozhodnutí, ktoré prijal príslušný orgán v súlade s vnútroštátnym právom.

2. Do 7. júna 2023 Komisia stanoví podrobný program na monitorovanie výstupov, výsledkov a vplyvov tohto nariadenia. V tomto programe monitorovania sa stanovia ukazovatele a spôsob získavania údajov a ďalších potrebných dôkazov, ako aj interval ich získavania. Uvedú sa v ňom kroky, ktoré majú Komisia a členské štáty podniknúť pri získavaní a analýze údajov a iných dôkazov na monitorovanie pokroku a hodnotenie tohto nariadenia podľa článku 23.

Článok 22

Správa o vykonávaní

Do 7. júna 2023 predloží Komisia Európskemu parlamentu a Rade správu o uplatňovaní tohto nariadenia. V tejto správe sa uvedú 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

Do 7. júna 2024 Komisia vykoná hodnotenie tohto nariadenia a predloží Európskemu parlamentu a Rade správu o jeho uplatňovaní, ktorá zahŕňa:

a) fungovanie a účinnosť mechanizmov záruk, najmä tých, ktoré sú stanovené v článku 4 ods. 4, článku 6 ods. 3 a článkoch 7 až 11;

b) vplyv uplatňovania tohto nariadenia na základné práva, najmä na slobodu prejavu a právo na informácie, rešpektovanie súkromného života a ochranu osobných údajov; a

c) príspevok tohto nariadenia k ochrane verejnej bezpečnosti.

K tejto správe sa podľa potreby pripoja legislatívne návrhy.

Členské štáty poskytnú Komisii informácie potrebné na vypracovanie tejto správy.

Komisia tiež posúdi potrebu a uskutočniteľnosť zriadenia európskej platformy pre teroristický obsah online na účely uľahčenia komunikácie a spolupráce podľa tohto nariadenia.

Článok 24

Nadobudnutie účinnosti a uplatňovanie

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

Uplatňuje sa od 7. júna 2022.

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

V Bruseli 29. apríla 2021

Za Európsky parlament	*Za Radu*
predseda	*predseda*
D.M. SASSOLI	A.P. ZACARIAS

PRÍLOHA I

PRÍKAZ NA ODSTRÁNENIE

(článok 3 nariadenia Európskeho parlamentu a Rady (EÚ) 2021/784)

Podľa článku 3 nariadenia (EÚ) 2021/784 (ďalej len „nariadenie“) adresát tohto príkazu na odstránenie odstráni teroristický obsah alebo znemožní prístup k teroristickému obsahu vo všetkých členských štátoch čo najskôr, ale v každom prípade do jednej hodiny od doručenia príkazu na odstránenie.

Podľa článku 6 nariadenia musí adresát uchovávať obsah a súvisiace údaje, ktoré boli odstránené alebo ku ktorým bol znemožnený prístup, počas šiestich mesiacov alebo na žiadosť príslušných orgánov alebo súdov aj dlhšie.

Podľa článku 15 ods. 2 nariadenia tento príkaz na odstránenie sa zašle v jednom z jazykov, ktoré určil adresát.

ODDIEL A:

Členský štát vydávajúceho príslušného orgánu:

.....

Pozn.: údaje o vydávajúcom príslušnom orgáne sa uvádzajú v oddiele E a F

Adresát a prípadne právny zástupca:

.....

Kontaktné miesto:

.....

Členský štát, v ktorom má poskytovateľ hostingových služieb hlavne miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právnych zástupca:

.....

Čas a dátum vydania príkazu na odstránenie:

.....

Referenčné číslo príkazu na odstránenie:

.....

ODDIEL B: Teroristický obsah, ktorý sa má odstrániť alebo ku ktorému sa má znemožniť prístup vo všetkých členských štátoch čo najskôr, ale v každom prípade do jednej hodiny od doručenia príkazu na odstránenie:

URL a akékoľvek ďalšie informácie umožňujúce identifikáciu a presnú lokalizáciu teroristického obsahu:

.....

Dôvody, prečo sa materiál považuje za teroristický obsah v súlade s článkom 2 bodom 7 nariadenia.

Materiál (zaškrtnite príslušnú(-é) možnosť(-i)):

☐ nabáda ostatných na spáchanie trestných činov terorizmu, ako je glorifikácia teroristických činov, obhajovanie spáchania takýchto činov (článok 2 bod 7 písm. a) nariadenia)

☐ nabáda ostatných na spáchanie alebo na podporu spáchania trestných činov terorizmu (článok 2 bod 7 písm. b) nariadenia)

☐ podnecuje ostatných na účasť na činnostiach teroristickej skupiny (článok 2 bod 7 písm. c) nariadenia)

☐ poskytuje návod na výrobu alebo použitie výbušnín, strelných zbraní alebo iných zbraní, alebo škodlivých alebo nebezpečných látok, alebo iných osobitných metód alebo techník na účely spáchania alebo podpory spáchania trestných činov terorizmu (článok 2 bod 7 písm. d) nariadenia)

☐ vytvára hrozbu spáchania niektorého z trestných činov terorizmu (článok 2 bod 7 písm. e) nariadenia).

Ďalšie informácie, pre ktoré sa materiál považuje za teroristický obsah:

.....

.....

.....

ODDIEL C: Informácie pre poskytovateľa obsahu

Upozorňujeme Vás, že (ak sa uplatňuje, zaškrtnite):

☐ z dôvodov verejnej bezpečnosti adresát **nesmie informovať poskytovateľa obsahu** o odstránení teroristického obsahu alebo znemožnení prístupu k nemu.

Ak sa neuplatňuje, pozrite oddiel G pre podrobné informácie o možnosti napadnúť príkaz na odstránenie v členskom štáte vydávajúceho príslušného orgánu podľa vnútroštátneho práva (kópia príkazu na odstránenie sa musí poslať poskytovateľovi obsahu, ak o to požiada).

ODDIEL D: Informácie príslušnému orgánu členského štátu, v ktorom má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca

Zaškrtnite príslušnú(-é) možnosť(-i):

☐ členský štát, v ktorom má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca, sa líši od členského štátu vydávajúceho príslušného orgánu

☐ kópia príkazu na odstránenie sa zasiela príslušnému orgánu členského štátu, v ktorom má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca

ODDIEL E: Údaje o vydávajúcom príslušnom orgáne

Druh (zaškrtnite príslušnú možnosť):

☐ sudca, súd alebo vyšetrujúci sudca

☐ orgán presadzovania práva

☐ iný príslušný orgán → vyplňte aj oddiel F

Údaje o vydávajúcom príslušnom orgáne alebo jeho zástupcovi, ktorý osvedčuje presnosť a správnosť príkazu na odstránenie:

Názov vydávajúceho príslušného orgánu:

.....

Meno jeho zástupcu a pracovná pozícia (titul a funkcia:

.....

Č. spisu:

.....

Adresa:

.....

Tel. číslo (medzinárodná predvoľba) (miestna predvoľba):

.....

Faxové číslo (medzinárodná predvoľba) (miestna predvoľba):

.....

E-mailová adresa .....

Dátum.....

Odtlačok úradnej pečiatky (ak je k dispozícii) a podpis ([1]):

.....

([1]) Podpis nie je nevyhnutný, ak sa príkaz na odstránenie zasiela cez autentifikované kanály na predkladanie písomností, ktoré môžu zaručiť pravosť príkazu na odstránenie.

ODDIEL F: Kontaktné údaje na účely nadväzujúcich krokov

Kontaktné údaje vydávajúceho príslušného orgánu na účely spätnej väzby o čase odstránenia alebo znemožnenia prístupu alebo na účely poskytnutia dodatočného objasnenia:

.....

Kontaktné údaje príslušného orgánu členského štátu, v ktorom má poskytovateľ hostingových služieb hlavné miesto podnikateľskej činnosti, alebo v ktorom má pobyt alebo je usadený jeho právny zástupca:

.....

ODDIEL G: Informácie o možných prostriedkoch nápravy

Informácie o príslušnom orgáne alebo súde, lehotách a postupoch v prípade napadnutia príkazu na odstránenie:

Príslušný orgán alebo súd, na ktorom možno napadnúť príkaz na odstránenie:

.....

Lehota pre napadnutie príkazu na odstránenie (dní/mesiacov od):

.....

Odkaz na ustanovenia vnútroštátnych právnych predpisov:

.....

PRÍLOHA II

FORMULÁR SPÄTNEJ VÄZBY PO ODSTRÁNENÍ TERORISTICKÉHO OBSAHU ALEBO ZNEMOŽNENÍ PRÍSTUPU K NEMU

(článok 3 ods. 6 nariadenia Európskeho parlamentu a Rady (EÚ) 2021/784)

ODDIEL A:

Adresát príkazu na odstránenie:

.....

Príslušný orgán, ktorý vydal príkaz na odstránenie:

.....

Číslo spisu príslušného orgánu, ktorý vydal príkaz na odstránenie:

.....

Číslo spisu adresáta:

.....

Čas a dátum doručenia príkazu na odstránenie:

.....

ODDIEL B: Opatrenia prijaté na splnenie príkazu na odstránenie

(zaškrtnite príslušnú možnosť):

☐ teroristický obsah bol odstránený

☐ prístup k teroristickému obsahu bol znemožnený vo všetkých členských štátoch

Čas a dátum prijatého opatrenia:

.....

ODDIEL C: Údaje o adresátovi

Názov poskytovateľa hostingových služieb:

.....

ALEBO

Meno právneho zástupcu poskytovateľa hostingových služieb:

.....

Členský štát, v ktorom sa nachádza hlavné miesto podnikateľskej činnosti poskytovateľa hostingových služieb:

.....

ALEBO

Členský štát, v ktorom má pobyt alebo je usadený právny zástupca poskytovateľa hostingových služieb:

.....

Meno oprávnenej osoby:

.....

E-mail: kontaktného miesta:

.....

Dátum:

.....

PRÍLOHA III

INFORMÁCIE O NEMOŽNOSTI VYKONAŤ PRÍKAZ NA ODSTRÁNENIE

(článok 3 ods. 7 a 8 nariadenia Európskeho parlamentu a Rady (EÚ) 2021/784)

ODDIEL A:

Adresát príkazu na odstránenie:

.....

Príslušný orgán, ktorý vydal príkaz na odstránenie:

.....

Číslo spisu príslušného orgánu, ktorý vydal príkaz na odstránenie:

.....

Číslo spisu adresáta:

.....

Čas a dátum doručenia príkazu na odstránenie:

.....

ODDIEL B: Nevykonanie príkazu:

1. Príkaz na odstránenie nemožno vykonať v lehote z týchto dôvodov (zaškrtnite príslušnú(-é) možnosť(-i)):

☐ vyššia moc alebo faktická nemožnosť, ktorú nezavinil poskytovateľ hostingových služieb vrátane objektívne odôvodniteľných technických alebo operačných dôvodov

☐ príkaz na odstránenie obsahuje zjavné chyby

☐ príkaz na odstránenie neobsahuje dostatočné informácie

2. Uveďte viac informácií o dôvodoch nevykonania príkazu:

.....

3. Ak príkaz na odstránenie obsahuje zjavné chyby a/alebo neobsahuje dostatočné informácie, uveďte chyby a ďalšie potrebné informácie alebo objasnenia:

.....

ODDIEL C: Údaje o poskytovateľovi hostingových služieb alebo jeho právnom zástupcovi

Názov poskytovateľa hostingových služieb:

.....

ALEBO

Meno právneho zástupcu poskytovateľa hostingových služieb:

.....

Meno oprávnenej osoby:

.....

Kontaktné údaje (e-mailová adresa):

.....

Podpis:

.....

Čas a dátum

.....