Rada
Evropské unie

Brusel 7. prosince 2018
(OR. en)

15336/18

Interinstitucionální spis:
2018/0331(COD)

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

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Datum:	6. prosince 2018
Příjemce:	Delegace
Č. předchozího dokumentu:	14978/18 + COR 1
Č. dok. Komise:	12129/18 + ADD 1-3
Předmět:	Návrh nařízení Evropského parlamentu a Rady o prevenci šíření teroristického obsahu online – obecný přístup

Na zasedání dne 6. prosince 2018 se Rada dohodla na obecném přístupu uvedeném v příloze.

Změny oproti návrhu Komise jsou vyznačeny ***tučnou kurzívou*** v případě nově doplněného textu a znakem […] v případě textu vypuštěného.

PŘÍLOHA

[…]

[…] ***Návrh***

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o prevenci šíření teroristického obsahu online

[…]

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výbor[1],

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Cílem tohoto nařízení je prostřednictvím prevence zneužívání hostingových služeb pro teroristické účely zajistit řádné fungování jednotného digitálního trhu v otevřené a demokratické společnosti. Fungování jednotného digitálního trhu je nutné zlepšovat posilováním právní jistoty ve prospěch poskytovatelů hostingových služeb, posilováním důvěry uživatelů v internetové prostředí a posilováním ochranných opatření ve smyslu svobody projevu a informací.

[1] Úř. věst. C , , s. .

(2) Aktivní poskytovatelé hostingových služeb na internetu hrají v digitální ekonomice důležitou roli, protože zajišťují spojení mezi podniky a občany, zprostředkovávají veřejnou diskuzi, distribuci a příjem informací, názorů a myšlenek a významně přispívají k inovacím, ekonomickému růstu a tvorbě pracovních míst v Unii. Jejich služby jsou však v některých případech zneužívány třetími stranami k provádění nezákonné činnosti online. Velké znepokojení vzbuzuje zneužívání poskytovatelů hostingových služeb teroristickými skupinami a jejich příznivci k šíření teroristického obsahu online za účelem šíření jejich informací, radikalizace, náboru, napomáhání a řízení teroristické činnosti.

(3) Přítomnost teroristického obsahu online má závažné negativní dopady na uživatele, občany a celou společnost, ale také na poskytovatele internetových služeb, na jejichž platformách se takový obsah nachází, neboť se tím narušuje důvěra jejich uživatelů a dochází poškozování jejich obchodních modelů. Vzhledem k tomu, že poskytovatelé online služeb hrají ústřední úlohu a mají k dispozici technologické prostředky a kapacity související s poskytovanými službami, nesou zvláštní společenskou odpovědnost za ochranu svých služeb před zneužitím teroristy a za boj proti teroristickému obsahu šířenému prostřednictvím jejich služeb.

(4) Abychom mohli omezit dostupnost teroristického obsahu online a náležitě řešit tento rychle se rozvíjející problém, je třeba doplnit úsilí v boji proti teroristickému obsahu online zahájené na úrovni Unie v roce 2015 v rámci dobrovolné spolupráce mezi členskými státy a poskytovateli hostingových služeb o jasný legislativní rámec. Legislativní rámec se snaží navázat na dobrovolné úsilí, které bylo posíleno doporučením Komise (EU) 2018/334[2], a reaguje na výzvy Evropského parlamentu, aby byla zintenzivněna opatření pro boj proti nezákonnému a škodlivému obsahu, a Evropské rady, aby došlo ke zlepšení automatického odhalování a odstraňování obsahu, jenž podněcuje k teroristickým činům.

[2] Doporučení Komise (EU) 2018/334 ze dne 1. března 2018 o opatřeních pro efektivní boj proti nezákonnému obsahu online (Úř. věst. L 63, 6.3.2018, p. 50).

(5) Uplatňováním tohoto nařízení by nemělo být dotčeno uplatňování článku 14 směrnice 2000/31/ES[3]. Opatření přijatá poskytovateli hostingových služeb v souladu s tímto nařízením, a to včetně proaktivních opatření, nesmí sama o sobě vést k tomu, že se na poskytovatele služeb přestane vztahovat výjimka z odpovědnosti stanovená příslušným ustanovením. Tímto nařízením nejsou dotčeny pravomoci vnitrostátních orgánů a soudů stanovit v konkrétních případech, kdy nejsou splněny podmínky pro výjimku z odpovědnosti dle článku 14 směrnice 2000/31/ES, odpovědnost poskytovatelů hostingových služeb. ***Toto nařízení se nevztahuje na činnosti související s národní bezpečností, neboť národní bezpečnost zůstává výhradní odpovědností každého členského státu.***

(6) Pravidla prevence zneužívání hostingových služeb k šíření teroristického obsahu online, jež mají zajistit řádné fungování vnitřního trhu, jsou stanovena v nařízení za plného respektování základních práv chráněných právním řádem Unie a zejména práv, která zaručuje Listina základních práv Evropské unie.

[3] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu) (Úř. věst. L 178, 17.7.2000, s. 1).

(7) Toto nařízení přispívá k ochraně veřejné bezpečnosti a současně stanoví náležitá a účinná ochranná opatření s cílem zajistit ochranu dotčených základních práv. Ta zahrnují práva na ochranu soukromí a osobních údajů, právo na účinnou soudní ochranu, právo na svobodu projevu, a to včetně práva přijímat a rozšiřovat informace, práva na svobodu podnikání a zásady zákazu diskriminace. Příslušné orgány a poskytovatelé hostingových služeb musí přijímat pouze taková opatření, která jsou nutná, vhodná a přiměřená v demokratické společnosti, a to s ohledem na velký význam svobody projevu a informací, ***jakož i svobodu tisku a pluralitu sdělovacích prostředků,*** která představuje […] […] základní pilíř pluralitní demokratické společnosti a je jednou z hodnot, na kterých byla Unie založena. Je nutné přísně zacílit na opatření, která by představovala zasahování do svobody projevu a informací, a to v tom smyslu, že musí sloužit k prevenci šíření teroristického obsahu, ovšem aniž by tím ovlivňovala právo přijímat a rozšiřovat informace, a zohlednit též ústřední úlohu, kterou poskytovatelé hostingových služeb hrají při zprostředkování veřejné diskuse, šíření a přijímání faktů, názorů a myšlenek v souladu se zákonem.

(8) Právo na účinnou právní ochranu je zakotveno v článku 19 Smlouvy o EU a článku 47 Listiny základních práv Evropské unie. Každá fyzická nebo právnická osoba má právo u příslušného vnitrostátního soudu na účinnou právní ochranu před opatřeními přijatými dle tohoto nařízení, která mají negativní dopady na práva takové osoby. Toto právo zahrnuje zejména možnost poskytovatelů hostingových služeb a poskytovatelů obsahu se účinně bránit proti příkazům k odstranění obsahu u soudu členského státu, ve kterém orgány příkaz k odstranění obsahu vydaly, ***a možnost poskytovatelů hostingových služeb bránit se proti rozhodnutí o uložení proaktivních opatření či sankcí u soudu členského státu, v němž mají sídlo nebo právního zástupce.***

(9) Aby se vyjasnilo, jaká opatření mají poskytovatelé hostingových služeb a příslušné orgány přijmout za účelem prevence šíření teroristického obsahu online, musí toto nařízení stanovit definici teroristického obsahu pro preventivní účely, která bude čerpat z definice teroristických trestných činů uvedené ve směrnici Evropského parlamentu a Rady (EU) 2017/541[4]. S ohledem na nutnost řešit nejškodlivější teroristickou propagandu na internetu musí definice postihovat materiál […], který podněcuje, podporuje a obhajuje páchání teroristických trestných činů nebo podílení se na nich, […] nebo propaguje účast na činnostech teroristické skupiny. […] ***Tato definice zahrnuje obsah, který poskytuje instrukce pro výrobu a použití výbušnin, palných nebo jiných zbraní nebo škodlivých či nebezpečných látek, jakož i chemických, biologických, radiologických a jaderných látek, nebo pokyny týkající se jiných metod a technik, včetně výběru cílů, za účelem spáchání teroristických trestných činů.*** Takový ***materiál*** […] zahrnuje zejména text, obrázky, zvukové nahrávky a videa. Při posuzování, zda je obsah teroristický ve smyslu tohoto nařízení, musí příslušné orgány i poskytovatelé hostingových služeb zohlednit faktory jako např. povahu a znění příslušného výroku či projevu, kontext, ve kterém byl učiněn, a jeho potenciál přivodit škodlivé důsledky, které by měly vliv na bezpečnost osob. Skutečnost, že byl materiál vytvořen teroristickou organizací nebo osobou uvedenou na příslušných seznamech EU, lze jej takové organizaci přičítat nebo je šířen jejím jménem, je při posouzení důležitým faktorem. Obsah šířený pro vzdělávací, […] ***protiargumentační*** či výzkumné účely je třeba náležitě chránit ***a dosáhnout přitom vhodné rovnováhy mezi základními právy, kam patří zejména svoboda projevu a informací, a potřebami veřejné bezpečnosti. Pokud za zveřejnění šířeného materiálu nese redakční odpovědnost poskytovatel obsahu, zohlední se v rámci jakéhokoli rozhodnutí týkajícího se odstranění tohoto obsahu standardy novinářské práce zakotvené v předpisech upravujících oblast tisku či sdělovacích prostředků, jež jsou v souladu s právem Unie, a právo na svobodu projevu a právo na svobodu a pluralitu sdělovacích prostředků podle článku 11 Listiny základních práv.*** Navíc by mělo být za teroristický obsah považováno vyjadřování radikálních, polemických či kontroverzních názorů ve veřejné diskuzi o citlivých politických otázkách.

---

[4] Směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV (Úř. věst. L 88, 31.3.2017, s. 6).

(10) Má-li se toto opatření vztahovat také na online hostingové služby, ve kterých je šířen teroristický obsah, mělo by toto nařízení upravovat služby informační společnosti, které uchovávají informace ***a materiál*** poskytované příjemcem služby na jeho žádost a které takové uchovávané informace ***a materiál*** zpřístupňují třetím stranám bez ohledu na to, zda je taková činnost pouze technické, automatické a pasivní povahy. […] ***Uchovávání obsahu spočívá v držení dat uložených v paměti fyzického nebo virtuálního serveru; tím jsou z oblasti působnosti vyňaty prosté přenosy a jiné služby elektronických komunikací ve smyslu [evropského kodexu pro elektronické komunikace] nebo poskytovatelé služeb ukládání do vyrovnávací paměti (caching), nebo jiné služby poskytované v jiných vrstvách internetové infrastruktury, např. registry a elektronické podatelny domén, DNS (systém doménových jmen) nebo související služby, jako jsou platební služby nebo služby ochrany před distribuovaným odepřením služby (DDoS). Navíc musejí být informace uloženy na žádost poskytovatele obsahu; do oblasti působnosti spadají pouze ty služby, v jejichž případě je poskytovatel obsahu přímým příjemcem. V neposlední řadě jsou uchovávané informace zpřístupněny třetím stranám, jimiž se rozumí jakýkoli třetí uživatel, který není poskytovatelem obsahu. Do oblasti působnosti nepatří interpersonální komunikační služby, které umožňují přímou interpersonální a interaktivní výměnu informací mezi konečným počtem osob, kdy osoby, které komunikaci zahajují nebo se jí účastní, určují jejího/její příjemce.*** Takoví poskytovatelé ***hostingových služeb*** […] například zahrnují platformy sociálních médií, služby audiovizuálního přenosu prostřednictvím internetu (tzv. video streaming), služby sdílení videa, obrazového a zvukového materiálu, služby sdílení souborů a jiné cloudové služby a ***služby ukládání obsahu*** […]. ***Toto nařízení se vztahuje na poskytování hostingových služeb, a nikoli na konkrétního poskytovatele nebo jeho dominantní činnost, která může spojovat hostingové služby s jinými službami, které nejsou v oblasti působnosti tohoto nařízení.***

(10a) Nařízení by se mělo také vztahovat na poskytovatele hostingových služeb s provozovnou mimo Unii, kteří ovšem nabízejí služby v rámci Unie, protože velká část poskytovatelů hostingových služeb vystavených v rámci svých služeb teroristickému obsahu online sídlí ve třetích zemích. To by mělo zajistit, že všechny společnosti působící na jednotném digitálním trhu splňují stejné požadavky, a to bez ohledu na zemi, kde mají provozovnu. K určení, zda poskytovatel služeb nabízí služby v Unii, je nutné posoudit, zda poskytovatel služeb umožňuje právnickým nebo fyzickým osobám v jednom či více členských státech využívat jeho služby. Avšak pouhá dostupnost webové stránky, e-mailové adresy a jiných kontaktních údajů poskytovatele služeb v jednom nebo více členských státech, posuzovaných odděleně, by neměla být dostatečnou podmínkou pro použití tohoto nařízení.

(11) Pro stanovení působnosti tohoto nařízení musí být relevantní podstatné spojení s Unií. Existence takového podstatného spojení s Unií se předpokládá tehdy, má-li poskytovatel služeb provozovnu v Unii, nebo, v případě absence provozovny, na základě existence významného počtu uživatelů v jednom nebo více členských státech nebo zacílení činností na jeden nebo více členských států. Zacílení činností na jeden nebo více členských států lze určit na základě všech relevantních okolností, včetně takových faktorů, jako je používání jazyka či měny obecně používaných v daném členském státě nebo možnost objednání zboží či služeb. Zacílení činností na některý členský stát by mohlo být též odvozeno od dostupnosti aplikace v obchodě s aplikacemi příslušného členského státu, od poskytování místních reklam nebo reklam v jazyce používaném v příslušném členském státě nebo od řešení vztahů se zákazníky, např. poskytováním zákaznického servisu v jazyce obecně používaném v příslušném členském státě. Podstatné spojení je třeba předpokládat i v případě, že poskytovatel služeb zaměřuje svoje činnosti na jeden nebo více členských států, jak stanoví čl. 17 odst. 1 písm. c) nařízení Evropského parlamentu a Rady č. 1215/2012[5]. Na druhou stranu poskytování služby s cílem pouhého souladu se zákazem diskriminace stanoveným v nařízení Evropského parlamentu a Rady (EU) 2018/302[6] nelze jen na základě tohoto důvodu pokládat za zaměření nebo zacílení činností na dané území v Unii.

---

[5] Nařízení Evropského parlamentu a Rady (EU) č. 1215/2012 ze dne 12. prosince 2012 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech (Úř. věst. L 351, 20.12.2012, str. 1).

[6] Nařízení Evropského parlamentu a Rady (EU) 2018/302 ze dne 28. února 2018 o řešení neoprávněného zeměpisného blokování a dalších forem diskriminace založených na státní příslušnosti, místě bydliště či místě usazení zákazníků v rámci vnitřního trhu a o změně nařízení (ES) č. 2006/2004 a (EU) 2017/2394 a směrnice 2009/22/ES (Úř. věst. L 601, 2.3.2018, str. 1).

(12) Poskytovatelé hostingových služeb musí plnit určité povinnosti náležité péče, aby zajistili prevenci šíření teroristického obsahu ve svých službách. Tyto povinnosti náležité péče by neměly představovat obecnou povinnost dohledu. Povinnosti náležité péče by měly při uplatňování tohoto nařízení zahrnovat požadavek, aby poskytovatelé hostingových služeb jednali ohledně uchovávaného obsahu s řádnou péčí a přiměřeně, a to zejména při uplatňování jejich vlastních podmínek s cílem zabránit odstranění obsahu, který není teroristickým ***obsahem***. Odebrání či zamezení přístupu musí být provedeno s ohledem na zajištění svobody projevu a informací.

(13) Je nutné harmonizovat postup a povinnosti vyplývající ze zákonných příkazů, které po posouzení příslušnými orgány, vyžadují po poskytovatelích hostingových služeb odstranit teroristický obsah nebo zamezit přístupu k němu. Členské státy budou mít volnost, co se týče výběru příslušných orgánů, a tento úkol budou moci uložit správním, donucovacím či soudním orgánům. S ohledem na rychlost šíření teroristického obsahu napříč online službami ukládá toto ustanovení poskytovatelům hostingových služeb povinnost zajistit, aby byl teroristický obsah uvedený v příkazu k odstranění obsahu odstraněn nebo přístup k němu zamezen od jedné hodiny od přijetí příkazu k odstranění obsahu. ***Aniž je dotčen požadavek na uchovávání údajů podle článku 7 tohoto nařízení nebo podle [návrhu právních předpisů v oblasti elektronických důkazů],*** je na poskytovateli hostingových služeb, aby rozhodl, zda dotyčný obsah odstraní, nebo zda k němu znemožní přístup uživatelům v Unii. ***V důsledku by tak měl poskytovatel zabránit uživatelům internetu, kteří využívají jeho služeb, v přístupu k obsahu, k němuž byl přístup znemožněn, nebo jim tento přístup přinejmenším ztížit a důrazně je od něj odradit.***

(13a) Příkaz k odstranění obsahu by měl zahrnovat klasifikaci příslušného obsahu jako obsahu teroristického a obsahovat informace dostatečné pro lokalizaci obsahu poskytnutím adresy URL a veškerých dalších doplňujících informací, jako je například snímek obrazovky zachycující daný obsah. Příslušný orgán by měl na žádost poskytnout doplňující odůvodnění, proč je obsah považován za teroristický. Odůvodnění nemusí obsahovat citlivé informace, které by mohly ohrozit vyšetřování. Odůvodnění by však mělo poskytovateli hostingových služeb, a v důsledku i poskytovateli obsahu umožnit, aby účinně vykonávali své právo na soudní nápravu.

(14) Příslušný orgán by měl příkaz k odstranění obsahu předat přímo adresátovi a kontaktnímu místu elektronickými prostředky umožňujícími vyhotovení písemného záznamu za podmínek, jež poskytovateli služeb umožňují ověřit pravost, včetně přesnosti data a času odeslání a přijetí příkazu, např. zabezpečenou e-mailovou poštou a prostřednictvím platforem nebo jiných zabezpečených kanálů, včetně těch, které dá k dispozici poskytovatel služeb, a to v souladu s pravidly pro ochranu osobních údajů. Tento požadavek lze uspokojit zejména využitím kvalifikovaných služeb elektronického doporučeného doručování, jak stanoví nařízení Evropského parlamentu a Rady (EU) č. 910/2014[7].

[7] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. věst. L 257, 28.8.2014, str. 73).

(15) […] Mechanismus ***hlášení*** upozorňující poskytovatele hostingových služeb na informace ***a materiál***, které mohou být považovány za teroristický obsah, který poskytovateli hostingových služeb umožňuje posoudit slučitelnost **s** jeho vlastními podmínkami, ***představuje*** […] ***obzvláště účinný, rychlý a přiměřený způsob, jak poskytovatele hostingových služeb informovat o konkrétním obsahu v jejich službách*** […]. Důležité je, aby poskytovatelé hostingových služeb taková hlášení prioritně posoudili a poskytli rychlou zpětnou vazbu o přijatých opatřeních. Konečné rozhodnutí, zda odstranit obsah, protože není v souladu s jejich podmínkami, leží i nadále na poskytovateli hostingových služeb. Při provádění tohoto nařízení v souvislosti s hlášením zůstává mandát Europolu stanovený nařízením (EU) 2016/794[8] nedotčen.

(16) S ohledem na rozsah a rychlost potřebné pro efektivní odhalování a odstraňování teroristického obsahu, jsou zásadním prvkem v boji proti teroristickému obsahu online přiměřená proaktivní opatření a v některých případech i využívání automatizovaných prostředků. Poskytovatelé hostingových služeb musí za účelem omezení dostupnosti teroristického obsahu posoudit, zda je vhodné přijmout proaktivní opatření v závislosti na rizicích a míře expozice teroristickému obsahu a také s ohledem na dopady na práva třetích stran a informace ve veřejném zájmu. V důsledku toho by měli poskytovatelé hostingových služeb určit, jaká vhodná, účinná a přiměřená proaktivní opatření přijmout. Z tohoto požadavku by neměla vyplývat obecná povinnost dohledu. V kontextu tohoto posouzení neexistence příkazů k odstranění obsahu a hlášení adresovaných poskytovateli hostingových služeb indikuje nízké ***riziko nebo*** nízkou úroveň expozice teroristickému obsahu.

---

8 Nařízení Evropského parlamentu a Rady (EU) č. 2016/794 ze dne 11. května 2016 o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV (Úř. věst. L 135, 24.5.2016, str. 53).

(17) Při zavádění proaktivních opatření musí poskytovatelé hostingových služeb zajistit, aby bylo zachováno právo uživatelů na svobodu projevu a informace, a to včetně svobodného přijímání a šíření informací. Kromě zákonem stanovených požadavků, včetně legislativy na ochranu osobních údajů, musí poskytovatelé hostingových služeb jednat s náležitou péčí a v příslušných případech přijmout ochranná opatření, včetně lidského dohledu a kontroly, za účelem prevence neúmyslných a chybných rozhodnutí vedoucích k odstranění obsahu, který není teroristický. To má zvláštní význam zejména tehdy, používají-li poskytovatelé hostingových služeb k odhalování teroristického obsahu automatizované prostředky. Rozhodnutí použít automatizované prostředky, ať už učiněné samotným poskytovatelem hostingových služeb či na základě žádosti příslušného orgánu, musí být posouzeno s ohledem na spolehlivost použité technologie a následné dopady na základní práva.

(18) Abychom zajistili, že poskytovatelé hostingových služeb vystavení teroristickému obsahu uplatňují náležitá opatření za účelem prevence zneužívání jejich služeb, příslušné orgány musí poskytovatele hostingových služeb, kteří obdrželi pravomocný příkaz k odstranění obsahu, žádat, aby oznámili proaktivní opatření, která uplatnili. Ta mohou spočívat v opatřeních za účelem prevence opětovného nahrání teroristického obsahu, odstranění obsahu nebo zamezení přístupu k němu v důsledku přijatého příkazu k odstranění obsahu nebo hlášení, a to za využití veřejných či soukromých nástrojů obsahujících známý teroristický obsah. Využívat mohou také spolehlivé technické nástroje určené k odhalování nového teroristického obsahu, ať už pomocí nástrojů dostupných na trhu nebo vyvinutých samotným poskytovatelem hostingových služeb. Poskytovatel služeb musí hlásit konkrétní uplatňovaná proaktivní opatření, aby mohl příslušný orgán posoudit, zda jsou opatření účinná a přiměřená a zda, jsou-li využívány automatizované prostředky, má poskytovatel hostingových služeb k dispozici nezbytné schopnosti lidského dohledu a kontroly. Při posuzování účinnosti a proporcionality opatření musí příslušný orgán zohlednit relevantní parametry včetně počtu příkazů k odstranění obsahu a hlášení vydaných poskytovatelem, jeho ekonomické možnosti a dopady jeho služeb na šíření teroristického obsahu (např. zohlednění počtu uživatelů v rámci Unie).

(19) V návaznosti na žádost musí příslušný orgán zahájit s poskytovatelem hostingových služeb dialog o nezbytných proaktivních opatřeních, která je třeba přijmout. V nezbytných případech by měl příslušný orgán uložit přijetí náležitých, účinných a přiměřených proaktivních opatření, považuje-li vzhledem k rizikům přijatá opatření za nedostatečná. Rozhodnutí uložit taková konkrétní proaktivní opatření nesmí v zásadě vést k uložení obecné povinnosti dohledu, jak je stanoveno v článku 15 odst. 1 směrnice 2000/31/ES. S ohledem na obzvláště závažná rizika související s šířením teroristického obsahu by se mohla rozhodnutí přijatá příslušnými úřady na základě tohoto nařízení odchýlit od přístupu stanoveného v článku 15 odst. 1 směrnice 2000/31/ES, co se týče určitých konkrétních, cílených opatření, jejichž přijetí je nezbytné z důvodů nadřazených zájmů v oblasti veřejné bezpečnosti. Před přijetím takových rozhodnutí musí příslušný orgán dosáhnout přiměřené rovnováhy mezi cíli veřejného zájmu a dotčenými základními právy, a to zejména co se týče svobody projevu a informací a svobody podnikání, a uvést patřičné odůvodnění.

(20) Povinnost poskytovatelů hostingových služeb uchovávat odstraněný obsah a související údaje musí být uloženy pro konkrétní účely a časově omezeny na nezbytnou dobu. Požadavek na uchovávání je nutné rozšířit na související údaje a v rozsahu, ve kterém by jinak v důsledku odstranění dotyčného obsahu došlo ke ztrátě takových údajů. Související údaje mohou obsahovat např. „údaje o účastníkovi“, mezi něž patří zejména údaje týkající se totožnosti poskytovatele obsahu, ***„údaje o transakcích“ a*** [...] „údaje o přístupu“, například včetně údajů o datu a času použití poskytovatelem obsahu, nebo přihlášení ke službě či odhlášení z ní, společně s IP adresou přidělenou poskytovateli obsahu poskytovatelem služby přístupu na internet.

(21) Povinnost uchovávat obsah pro účely řízení správního či soudního přezkumu je nutná a důvodná s cílem zajištění účinných opatření soudní nápravy pro poskytovatele obsahu, jejichž obsah byl odstraněn nebo k němu byl zamezen přístup, a také zajištění obnovení takového obsahu do stavu, v jakém byl před odstraněním, v závislosti na výsledku přezkoumání. Tato povinnost uchovávat obsah pro účely vyšetřování a trestního stíhání je důvodná a nutná s ohledem na hodnotu, kterou může tento materiál přinést ve prospěch narušení či prevence teroristické činnosti. V případech, kdy společnosti odstraní materiál nebo zamezí přístupu k němu, a to zejména prostřednictvím vlastních proaktivních opatření, a neinformují o tom příslušné orgány, protože vyhodnotí, že nespadá do působnosti článku 13 odst. 4 tohoto nařízení, nemusí donucovací orgány o existenci takového obsahu vědět. Proto je uchovávání obsahu pro účely prevence, odhalování vyšetřování a trestního stíhání teroristických trestných činů také důvodné. Pro tyto účely je vyžadované uchovávání omezeno na údaje, které jsou pravděpodobně napojeny na teroristické trestné činy, a mohou tudíž přispívat k trestnímu stíhání teroristických trestných činů nebo prevenci závažných rizik vůči veřejné bezpečnosti.

(22) Aby byla zajištěna proporcionalita, musí být lhůta na uchování omezena na šest měsíců, aby měli poskytovatelé obsahu dostatečný čas na zahájení přezkumného řízení a donucovací orgány přístup k relevantním údajům pro účely vyšetřování a trestního stíhání teroristických trestných činů. Tato lhůta ovšem může být na žádost orgánu provádějícího přezkum prodloužena na dobu nezbytnou, pokud je přezkumné řízení zahájeno, ale není v rámci šestiměsíční lhůty dokončeno. Tato lhůta by měla být dostatečná, aby umožnila donucovacím orgánům zachovat nezbytné důkazy související s vyšetřováním a současně zajistit rovnováhu ve vztahu k dotčeným základním právům.

(23) Tímto nařízením nejsou dotčeny procesní záruky ani procesní vyšetřovací opatření vztahující se k přístupu k obsahu a souvisejícím údajům uchovávaným pro účely vyšetřování a trestního stíhání teroristických trestných činů, jak je stanoveno vnitrostátním právem členských států a právními předpisy Unie.

(24) Transparentnost pravidel poskytovatelů hostingových služeb ve vztahu k teroristickému obsahu je nezbytná pro posílení jejich odpovědnosti vůči uživatelům a důvěry občanů v jednotný digitální trh. Poskytovatelé hostingových služeb, ***kteří jsou vystaveni teroristickému obsahu,*** by měli jednou za rok zveřejňovat zprávy o transparentnosti obsahující smysluplné informace o opatřeních přijatých v souvislosti s odhalováním, identifikací a odstraňováním teroristického obsahu***, pokud to nemaří účel zavedených opatření***.

(25) Postupy řešení stížností představují nezbytné ochranné opatření proti chybnému odstranění obsahu***, v důsledku opatření přijatých podle podmínek poskytovatelů hostingových služeb,*** chráněného právem na svobodu projevu a informací. Poskytovatelé hostingových služeb proto musí zřídit uživatelsky vstřícné mechanismy pro podání stížností a zajistit, aby byly stížnosti řešeny neprodleně a zcela transparentně ve vztahu k poskytovateli obsahu. Požadavkem, aby poskytovatelé hostingových služeb obnovili obsah, který byl chybně odstraněn, není dotčena možnost prosazování vlastních podmínek poskytovatelů hostingových služeb na základě jiných důvodů. ***Kromě toho by poskytovatelé obsahu, jejichž obsah byl odstraněn v důsledku příkazu k odstranění, měli mít právo na účinnou právní ochranu v souladu s článkem 19 SEU a článkem 47 Listiny základních práv Evropské unie.***

(26) ***Obecněji řečeno ú***[…]činná právní ochrana dle článku 19 Smlouvy o EU a článku 47 Listiny základních práv Evropské unie vyžaduje, aby byly osoby schopny zjistit důvody, na základě kterých byl jimi nahraný obsah odstraněn nebo k němu byl zamezen přístup. Pro tento účel musí poskytovatel hostingových služeb poskytovateli obsahu zpřístupnit smysluplné informace, které poskytovateli obsahu umožní rozhodnutí zpochybnit. Toto ovšem nemusí nutně vyžadovat hlášení učiněné vůči poskytovateli obsahu. V závislosti na okolnostech mohou poskytovatelé hostingových služeb nahradit obsah, který je považován za teroristický obsah, sdělením, že byl obsah odstraněn nebo k němu zamezen přístup v souladu s tímto nařízením. Další informace o důvodech a možnostech zpochybnění rozhodnutí poskytovatelem obsahu budou předány na vyžádání. Rozhodnou-li se příslušné orgány, že z důvodu veřejné bezpečnosti, a to i v kontextu vyšetřování, je považováno za nevhodné či kontraproduktivní informovat o odstranění obsahu nebo zamezení přístupu k němu přímo poskytovatele služeb, pak musí informovat poskytovatele hostingových služeb.

(27) Aby se zabránilo duplikaci a případným zásahům do šetření, příslušné orgány by se měly […] ***před*** vydáním příkazů k odstranění obsahu či ***při*** zaslání hlášení poskytovatelům hostingových služeb vzájemně informovat, koordinovat činnosti a spolupracovat a v příslušných případech tak činit také ve spolupráci s Europolem. […] ***Při rozhodování o vydání příkazu k odstranění by měl příslušný orgán náležitě zohlednit jakékoli upozornění na zásah do zájmů šetření („sladění činností“). Je-li příslušný orgán informován příslušným orgánem jiného členského státu o existujícím příkazu k odstranění, neměl by vydávat příkaz duplicitní.*** Při provádění ustanovení tohoto nařízení může Europol poskytovat podporu v souladu s aktuálním mandátem a stávajícím právním rámcem.

(28) Za účelem zajištění účinného a dostatečně soudržného provádění proaktivních opatření musí příslušné orgány členských států vzájemně spolupracovat v oblasti dialogů vedených s poskytovateli hostingových služeb, co se týče identifikace, provádění a hodnocení konkrétních proaktivních opatření. Obdobně je taková spolupráce nutná také ve vztahu k přijetí pravidel týkajících se sankcí, jejich uplatňování a vymáhání. ***Komise by měla tuto koordinaci a spolupráci usnadňovat.***

(29) Je nezbytné, aby byly příslušné orgány členských států zodpovědné za ukládání sankcí v plném rozsahu informovány o vydávání příkazů k odstranění obsahu a hlášeních a následné komunikaci mezi poskytovatelem hostingových služeb a relevantním příslušným orgánem. Pro tento účel musí členské státy zajistit náležité komunikační kanály a mechanismy, které umožní včasné sdílení relevantních informací.

(30) Za účelem zprostředkování rychlé komunikace mezi příslušnými orgány a s poskytovateli hostingových služeb a prevence duplicitních činností se členské státy […] ***vybízejí***, aby využívaly ***specializované*** nástroje vyvinuté Europolem, jako např. stávající aplikaci pro správu hlášení obsahu na internetu (Internet Referral Management application, IRMa) nebo následně vyvinuté nástroje.

(31) S ohledem na obzvláště závažné důsledky některého teroristického obsahu musí poskytovatelé hostingových služeb o existenci jakýchkoliv důkazů o teroristických trestných činech, o kterých se dozví, neprodleně informovat orgány v dotčených členských státech nebo příslušné orgány v zemích, kde mají sídlo nebo právního zástupce. Za účelem zajištění proporcionality je tato povinnost omezena na teroristické trestné činy definované v článku 3 odst. 1 směrnice (EU) 2017/541. Z této oznamovací povinnosti nevyplývá povinnost poskytovatelů hostingových služeb takové důkazy aktivně vyhledávat. Dotčený členský stát je členský stát, který je příslušný pro vyšetřování a trestní stíhání teroristického trestného činu dle směrnice (EU) 2017/541 na základě národnosti pachatele nebo potenciální oběti trestného činu nebo cílové lokality teroristického činu. V případě pochybností mohou poskytovatelé hostingových služeb předat informace Europolu, který bude jednat na základě svého mandátu, a to včetně předání záležitosti relevantním vnitrostátním orgánům.

(32) Příslušné orgány v členských orgánech by měly mít možnost využívat takové informace k přijetí vyšetřovacích opatření dostupných v rámci právních předpisů členského státu nebo Unie, a to včetně evropského předávacího příkazu dle nařízení o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech[9].

(33) Poskytovatelé hostingových služeb i členské státy musí zřídit kontaktní místa, která umožní rychlé zpracování příkazů k odstranění obsahu a hlášení. Na rozdíl od právního zástupce slouží kontaktní místo k provozním účelům. Kontaktní místo poskytovatele hostingových služeb může spočívat ve vyhrazeném prostředku***, interním nebo externím***, který umožní elektronické podání příkazů k odstranění obsahu a hlášení, a technických […] ***nebo*** personálních prostředcích umožňujících jejich rychlé zpracování. Kontaktní místo poskytovatele hostingových služeb se nemusí nacházet v Unii a poskytovatel hostingových služeb má možnost určit stávající kontaktní místo, pokud je takové kontaktní místo schopno plnit funkce stanovené tímto nařízením. Aby mohl být teroristický obsah odstraněn nebo aby mohlo být zamezeno v přístupu k němu do jedné hodiny od přijetí příkazu k odstranění, ***poskytovatelé hostingových služeb, kteří byli vystaveni teroristickému obsahu, což dokládá přijetí příkazu k odstranění,*** musejí zajistit, že kontaktní místo bude dostupné 24 hodin denně, 7 dní v týdnu. Informace o kontaktním místě by měly zahrnovat informace o jazyce, ve kterém se lze na kontaktní místo obracet. Za účelem umožnění komunikace mezi poskytovateli hostingových služeb a příslušnými orgány nabádáme poskytovatele hostingových služeb, aby umožnili komunikaci v jednom z úředních jazyků Unie, ve kterém jsou dostupné jejich obchodní podmínky.

(34) Protože neexistuje požadavek, aby poskytovatelé služeb zajistili fyzickou přítomnost na území Unie, je nutné jednoznačně určit, do příslušnosti kterého členského státu spadá poskytovatel hostingových služeb nabízející služby v Unii. Obecně platí, že poskytovatel hostingových služeb spadá do příslušnosti členského státu, ve kterém má hlavní provozovnu nebo kde určil právního zástupce. ***Nicméně z důvodu účinného provádění, naléhavosti a veřejného pořádku by měl kterýkoli členský stát být příslušný, pokud jde o příkazy k odstranění a hlášení.***

---

[9] COM(2018) 225 final.

(35) Poskytovatelé hostingových služeb, kteří nemají provozovnu v Unii, musí písemně určit právního zástupce, aby zajistili plnění povinností stanovených tímto nařízením a jejich prosazování. ***Poskytovatelé hostingových služeb mohou využívat stávajícího právního zástupce za předpokladu, že tento právní zástupce je schopen plnit funkce stanovené v tomto nařízení.***

(36) Právní zástupce by měl být právně zmocněn, aby jednal jménem poskytovatele hostingových služeb.

(37) Pro účely tohoto nařízení musí členské státy určit příslušné orgány. Požadavek určit příslušné orgány nemusí nutně vyžadovat zřízení nových orgánů, ale uložení úkolů a funkcí stanovených tímto nařízením stávajícím orgánům. Toto nařízení vyžaduje určit orgány pověřené vydáváním příkazů k odstranění obsahu, hlášením, dohledem nad proaktivními opatřeními a ukládáním sankcí. Je na rozhodnutí členských států, kolik orgánů těmito úkoly pověří.

(38) Sankce jsou nezbytné k zajištění účinného provádění povinností dle tohoto nařízení poskytovateli hostingových služeb. Členské státy by měly přijmout pravidla pro sankce***, jež mohou být správní či trestní povahy,*** a to v příslušných případech včetně pokynů pro stanovení pokut. Obzvláště přísné sankce je třeba uplatňovat v případě, že poskytovatel hostingových služeb systematicky neplní povinnost odstraňovat teroristický obsah či zamezit přístupu k němu do jedné hodiny od přijetí příkazu k odstranění obsahu. Neplnění povinností v jednotlivých případech lze postihovat s ohledem na zásadu *ne bis in idem* a zásadu proporcionality a zajistit, že takové sankce zohledňují soustavné nedostatky. Za účelem zajištění právní jistoty musí nařízení stanovit, v jakém rozsahu mohou podléhat relevantní povinnosti sankcím. Sankce za neplnění článku 6 by měly být uplatněny ve vztahu k povinnostem vyplývajícím z žádosti o zprávu dle článku 6 odst. 2 nebo rozhodnutí o uložení dalších proaktivních opatření dle článku 6 odst. 4. ***Při posuzování povahy daného porušení a rozhodování o uplatnění sankcí by měla být plně respektována základní práva, jako je svoboda projevu.*** Při stanovení, zda uložit finanční postihy, je třeba náležitým způsobem zjistit finanční situaci poskytovatele. Členské státy musí zajistit, aby sankce nemotivovaly k odstraňování obsahu, který není teroristickým obsahem.

(39) Používání standardizovaných šablon umožňuje spolupráci a výměnu informací mezi příslušnými orgány a poskytovateli služeb a umožňuje jim rychlejší a efektivnější spolupráci. Obzvláště důležité je zajistit po přijetí příkazů k odstranění obsahu rychlou realizaci opatření. Šablony snižují náklady na překlad a přispívají k vysoké kvalitě. Obdobně tak formuláře odpovědí by měly umožnit standardizovanou výměnu informací, což bude obzvláště důležité v případech, kdy nejsou poskytovatelé služeb schopni zajistit soulad. Ověřené kanály pro hlášení zaručují autentičnost příkazů k odstranění obsahu, a to včetně přesnosti data a času odeslání a přijetí příkazu.

(40) Aby bylo možné v nezbytných případech provádět rychlé změny obsahu šablon, které budou sloužit pro účely tohoto nařízení, měla by být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování Evropské unie, aby mohla změnit přílohy I, II a III tohoto nařízení. Aby bylo možné zohlednit vývoj technologií a souvisejícího právního rámce, Komise by rovněž měla být zmocněna k přijímání aktů v přenesené pravomoci, aby toto nařízení mohla doplnit o technické požadavky na elektronické prostředky využívané příslušnými orgány k přenosu příkazů k odstranění obsahu. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě o zdokonalení tvorby právních předpisů ze dne 13. dubna 2016[10]. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států, přičemž jejich odborníci mají automaticky přístup na setkání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

(41) Členské státy musí shromažďovat informace o zavádění právních předpisů. ***Členské státy mohou využívat zprávy o transparentnosti od poskytovatelů hostingových služeb a v případě potřeby je doplnit o podrobnější informace.*** Za účelem získání informací pro hodnocení právního předpisu je nutné stanovit podrobný program monitorování výstupů, výsledků a dopadů tohoto nařízení.

[10] Úř. věst. L 123, 12.5.2016, str. 1.

(42) Na základě zjištění a závěrů prováděcí zprávy a výsledku monitorování by měla Komise provést hodnocení tohoto nařízení, a to až po třech letech od okamžiku, kdy nařízení vstoupí v platnost. Hodnocení by mělo být založeno na pěti kritériích efektivnosti, účinnosti, relevantnosti, soudržnosti a přidané hodnoty EU. Posoudí fungování různých provozních a technických opatření stanovených tímto nařízením, a to včetně účinnosti opatření pro zlepšení odhalování, identifikace a odstraňování teroristického obsahu a účinnosti ochranných mechanismů, a také dopady na potenciálně dotčená práva a zájmy třetích stran, a to včetně přezkumu požadavku informovat poskytovatele obsahu.

(43) Jelikož cíle tohoto nařízení, totiž zajištění řádného fungování jednotného digitálního trhu pomocí prevence šíření teroristického obsahu online, nemůže být uspokojivě dosaženo členskými státy, ale spíše jej z důvodu rozsahu a účinků činnosti lze lépe dosáhnout na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení tohoto cíle,

PŘIJALY TOTO NAŘÍZENÍ:

ODDÍL I
OBECNÁ USTANOVENÍ

Článek 1

Předmět a oblast působnosti

1. Toto nařízení stanoví jednotná pravidla pro prevenci zneužití hostingových služeb k šíření teroristického obsahu online. Stanoví zejména:

   a) pravidla týkající se povinností náležité péče, které mají poskytovatelé hostingových služeb uplatňovat s cílem zabránit šíření teroristického obsahu prostřednictvím jejich služeb a v případě potřeby zajistit jeho rychlé odstranění;

   b) soubor opatření, která mají členské státy zavést s cílem identifikovat teroristický obsah, umožnit, aby tento obsah poskytovatelé hostingových služeb rychle odstranili, a usnadnit spolupráci s příslušnými orgány v jiných členských státech, s poskytovateli hostingových služeb a případně s příslušnými subjekty Unie.

2. Toto nařízení se vztahuje na poskytovatele hostingových služeb, kteří nabízejí služby v Unii, bez ohledu na místo, kde má takový poskytovatel svou hlavní provozovnu.

3. ***Tímto nařízením není dotčena povinnost dodržovat základní práva a obecné právní zásady zakotvené v článku 6 Smlouvy o Evropské unii.***

Článek 2

Definice

Pro účely tohoto nařízení se rozumí:

(1) „poskytovatelem hostingových služeb“ poskytovatel služeb informační společnosti spočívajících v uchovávání informací poskytovaných poskytovatelem obsahu a na jeho žádost a ve zpřístupňování informací třetím stranám;

(2) „poskytovatelem obsahu“ uživatel, který poskytl informace, které jsou nebo byly na žádost uživatele uloženy poskytovatelem hostingových služeb;

(3) „poskytováním služeb v Unii“ umožnění právnickým nebo fyzickým osobám v jednom nebo více členských státech využívat služeb poskytovatele hostingových služeb, který má významné spojení s tímto členským státem nebo členskými státy, například: provozovnu poskytovatele hostingových služeb v Unii;

Při neexistenci takové provozovny vychází posouzení významného spojení z konkrétních skutečných kritérií, jako je

a) významný počet uživatelů v jednom nebo více členských států;

b) ***nebo*** zaměření činností na jeden nebo více členských státech.

(4) „teroristickým trestným činem“ ***některý z úmyslných činů vymezených*** [...] v čl. 3 odst. 1 […] směrnice (EU) 2017/541;

(5) „teroristickým obsahem“ […] ***materiál***, ***který může přispět ke spáchání úmyslných činů, jak jsou vymezeny v čl. 3 odst. 1 písm. a) až i) směrnice 2017/541 tím, že obsahuje***:

aa) vyhrožování spácháním teroristického trestného činu;

a) podněcování k […] páchání teroristických trestných činů, nebo jejich obhajování, ***jako je*** […] ***jejich glorifikace***, představující riziko, že takové činy budou spáchány;

b) ***vybízení osob nebo skupiny osob k páchání*** […] […] teroristických trestných činů nebo k přispívání k nim;

c) podporu činností teroristické skupiny, zejména ***vybízení osob nebo skupiny osob k*** účasti na ***trestné činnosti*** teroristické skupiny či k její podpoře ve smyslu čl. 2 odst. 3 směrnice (EU) 2017/541;

pokyny týkající se metod či technik za účelem spáchání teroristických trestných činů.

(6) „šířením teroristického obsahu“ zpřístupnění teroristického obsahu třetím stranám prostřednictvím poskytovatelů hostingových služeb;

(7) „podmínkami“ všechny podmínky a ustanovení bez ohledu na jejich název nebo formu, které upravují smluvní vztah mezi poskytovatelem hostingových služeb a jejich uživateli;

(8) „hlášením“ oznámení příslušného orgánu nebo případně příslušného subjektu Unie poskytovateli hostingových služeb o informacích, které lze považovat za teroristický obsah, aby poskytovatel dobrovolně zvážil slučitelnost teroristického obsahu se svými vlastními podmínkami, a zabránilo se tak jeho šíření;

(9) „hlavní provozovnou“ ústředí nebo sídlo, v němž jsou vykonávány hlavní finanční funkce a provozní kontrola ***v rámci Unie***.

ODDÍL II

OPATŘENÍ PRO PREVENCI ŠÍŘENÍ TERORISTICKÉHO OBSAHU ONLINE

Článek 3

Povinnosti náležité péče

1. Poskytovatelé hostingových služeb přijímají v souladu s tímto nařízením vhodná, rozumná a přiměřená opatření, jejichž cílem je bojovat proti šíření teroristického obsahu a chránit před tímto obsahem uživatele. Přitom jednají řádně, přiměřeným a nediskriminačním způsobem a s patřičným ohledem na základní práva uživatelů a berou v úvahu zásadní význam svobody projevu a informací v otevřené a demokratické společnosti.

2. Poskytovatelé hostingových služeb zahrnou do svých podmínek ustanovení, ***že nebudou uchovávat teroristický obsah,*** a budou uplatňovat ustanovení zamezující šíření teroristického obsahu.

Článek 4

Příkazy k odstranění

1. Příslušný orgán je oprávněn vydat […] ***příkaz k odstranění***, kterým se od poskytovatele hostingových služeb požaduje, aby teroristický obsah odstranil nebo znemožnil přístup k němu.

2. Poskytovatelé hostingových služeb do jedné hodiny od přijetí příkazu k odstranění odstraní teroristický obsah nebo k němu znemožní přístup.

3. Příkazy k odstranění obsahují v souladu se vzorem uvedeným v příloze I tyto prvky:

   a) identifikaci příslušného orgánu, který vydává příkaz k odstranění, a autentizaci příkazu k odstranění ze strany příslušného orgánu; […] ***posouzení obsahu,*** přinejmenším prostřednictvím odkazu na ***příslušné*** kategorie teroristického obsahu uvedené v čl. 2 odst. 5;

b) jednotný lokátor zdroje (URL) a v případě potřeby další informace umožňující identifikaci uvedeného obsahu;

c) odkaz na toto nařízení jako právní základ pro příkaz k odstranění;

d) razítko s datem a časem vydání;

e) informace o opravných prostředcích, které má k dispozici poskytovatel hostingových služeb a poskytovatel obsahu;

f) rozhodnutí nezveřejnit informace o odstranění teroristického obsahu nebo o znemožnění přístupu k němu podle článku 11, je-li to relevantní.

4. Na žádost poskytovatele hostingových služeb nebo poskytovatele obsahu předloží příslušný orgán […] ***doplňující*** odůvodnění ***s vysvětlením, proč je obsah považován za teroristický***, aniž je dotčena povinnost poskytovatele hostingových služeb splnit příkaz k odstranění ve lhůtě stanovené v odstavci 2.

5. Příslušné orgány zašlou příkazy k odstranění do hlavní provozovny poskytovatele hostingových služeb nebo právnímu zástupci určenému poskytovatelem hostingových služeb podle článku 16 a předají ji kontaktnímu místu uvedenému v čl. 14 odst. 1. Tyto příkazy se zasílají elektronickými prostředky, které dovolují předložit písemný záznam za podmínek umožňujících autentizaci odesílatele, včetně přesnosti data a času odeslání a obdržení příkazu.

6. Poskytovatelé hostingových služeb ***bez zbytečného odkladu*** potvrdí přijetí příkazu a […] informují příslušný orgán o odstranění teroristického obsahu nebo o znemožnění přístupu k němu, přičemž uvedou zejména čas, kdy byl zásah proveden, a použijí k tomu šablonu uvedenou v příloze II.

7. Pokud poskytovatel hostingových služeb nemůže příkazu k odstranění vyhovět z důvodu vyšší moci nebo faktické nemožnosti, za kterou nenese vinu poskytovatel hostingových služeb, informuje tento bez zbytečného odkladu příslušný orgán a uvede důvody, a to za použití vzoru uvedeného v příloze III. Lhůta stanovená v odstavci 2 se uplatní, jakmile pominou uvedené důvody.

8. Pokud poskytovatel hostingových služeb nemůže příkazu k odstranění vyhovět, protože příkaz k odstranění obsahuje zjevné chyby nebo neobsahuje dostatečné informace pro jeho provedení, uvědomí o tom bez prodlení příslušný orgán a požádá o nezbytné vysvětlení za použití vzoru uvedeného v příloze III. Lhůta uvedená v odstavci 2 se uplatní, jakmile je vysvětlení poskytnuto.

9. Příslušný orgán, který vydal příkaz k odstranění, informuje příslušný orgán, který dohlíží na provádění proaktivních opatření uvedených v čl. 17 odst. 1 písm. c), jakmile příkaz k odstranění nabude konečnou platnost. Příkaz k odstranění nabývá konečnou platnost, pokud proti němu nebylo podáno odvolání ve lhůtě podle platného vnitrostátního práva, nebo pokud byl po podání odvolání potvrzen.

Článek 4a

Konzultační postup pro příkazy k odstranění

1. Vydávající orgán, který poskytovateli hostingových služeb zasílá příkaz k odstranění podle čl. 4 odst. 5, současně předloží kopii tohoto příkazu příslušnému orgánu podle čl. 17 odst. 1 písm. a) v členském státě, ve kterém má dotčený poskytovatel hostingových služeb hlavní provozovnu.

2. Má-li příslušný orgán členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu, přiměřené důvody se domnívat, že daný příkaz k odstranění může mít dopad na základní zájmy uvedeného členského státu, informuje o tom vydávající příslušný orgán.

3. Vydávající orgán tyto okolnosti zohlední a dle potřeby příkaz k odstranění stáhne nebo patřičně pozmění.

Článek 5

Hlášení

1. Příslušný orgán nebo příslušný subjekt Unie může zaslat hlášení poskytovateli hostingových služeb.

2. Poskytovatelé hostingových služeb zavedou provozní a technická opatření usnadňující rychlé posouzení obsahu, který jim příslušné orgány a případně příslušné subjekty Unie přeposlaly k jejich dobrovolnému posouzení.

3. Hlášení je adresováno do hlavní provozovny poskytovatele hostingových služeb nebo právnímu zástupci určenému poskytovatelem služeb podle článku 16 a předáno kontaktnímu místu uvedenému v čl. 14 odst. 1. Tato hlášení se zasílají elektronicky.

4. Hlášení obsahuje dostatek […] informací […] ***o*** důvodech, proč je obsah považován za teroristický, ***a uvede adresu*** URL a v případě potřeby doplňující informace umožňující identifikaci uvedeného teroristického obsahu.

5. Poskytovatel hostingových služeb posoudí přednostně obsah, který byl předmětem hlášení, podle svých podmínek a rozhodne, zda tento obsah odstraní nebo k němu znemožní přístup.

6. Poskytovatel hostingových služeb ***bez zbytečného odkladu*** […] informuje příslušný orgán nebo příslušný subjekt Unie o výsledku posouzení a o načasování opatření přijatých na základě hlášení.

7. Jestliže se poskytovatel hostingových služeb domnívá, že hlášení neobsahuje dostatečné informace pro posouzení uvedeného obsahu, neprodleně uvědomí příslušné orgány nebo příslušný subjekt Unie a uvede, jaké další informace nebo vysvětlení je třeba poskytnout.

Článek 6

Proaktivní opatření

1. Poskytovatelé hostingových služeb […] ***v závislosti na rizicích a míře expozice teroristickému obsahu*** přijmou proaktivní opatření na ochranu svých služeb proti šíření teroristického obsahu. Opatření musí být účinná a přiměřená s ohledem na riziko a míru expozice vůči teroristickému obsahu, základní práva uživatelů a zásadní význam svobody projevu a informací v otevřené a demokratické společnosti.

2. Jestliže byl příslušný orgán uvedený v čl. 17 odst. 1 písm. c) v souladu s čl. 4 odst. 9 informován, požádá poskytovatele hostingových služeb, aby do tří měsíců po obdržení žádosti a poté alespoň jednou ročně předložil zprávu o konkrétních proaktivních opatřeních, která přijal, a to i za použití automatizovaných nástrojů, za účelem:

   a) […] ***účinného řešení*** opětovného ***výskytu*** […] obsahu, který byl již dříve odstraněn nebo k němuž byl odepřen přístup, protože je považován za teroristický;

   b) zjištění, identifikace a urychleného odstranění teroristického obsahu či znemožnění přístupu k němu.

   Tato žádost musí být zaslána do hlavní provozovny poskytovatele hostingových služeb nebo právnímu zástupci určenému poskytovatelem služeb.

   Zprávy obsahují všechny relevantní informace, které umožní příslušnému orgánu uvedenému v čl. 17 odst. 1 písm. c) posoudit, zda jsou proaktivní opatření účinná a přiměřená, mimo jiné s cílem vyhodnotit fungování všech používaných automatizovaných nástrojů, jakož i lidský dohled a používané mechanismy pro ověřování.

3. Jestliže se příslušný orgán uvedený v čl. 17 odst. 1 písm. c) domnívá, že proaktivní opatření přijatá a nahlášená podle odstavce 2 nejsou dostatečná pro zmírnění a řízení rizika a úrovně expozice, může poskytovatele hostingových služeb požádat, aby přijal zvláštní dodatečná proaktivní opatření. Za tímto účelem spolupracuje poskytovatel hostingových služeb s příslušným orgánem uvedeným v čl. 17 odst. 1 písm. c) s cílem určit konkrétní opatření, která poskytovatel hostingových služeb zavede, a stanovit hlavní cíle a referenční hodnoty, jakož i lhůty pro jejich provedení.

4. Pokud do tří měsíců od podání žádosti podle odstavce 3 nelze dosáhnout dohody, může příslušný orgán uvedený v čl. 17 odst. 1 písm. c) vydat rozhodnutí, kterým se ukládají zvláštní dodatečná nezbytná a přiměřená proaktivní opatření. Rozhodnutí zohlední zejména finanční možnosti poskytovatele hostingových služeb a účinek takových opatření na základní práva uživatelů a zásadní význam svobody projevu a informací. ***Je na uvážení příslušného orgánu uvedeného v čl. 17 odst. 1 písm. c), aby rozhodl o povaze a rozsahu proaktivních opatření, v souladu s cílem tohoto nařízení.*** Toto rozhodnutí musí být zasláno do hlavní provozovny poskytovatele hostingových služeb nebo právnímu zástupci určenému poskytovatelem služeb. Poskytovatel hostingových služeb o provádění těchto opatření stanovených příslušným orgánem uvedeným v čl. 17 odst. 1 písm. c) pravidelně podává zprávy.

5. Poskytovatel hostingových služeb může kdykoli požádat příslušný orgán uvedený v čl. 17 odst. 1 písm. c), aby záležitost přezkoumal a žádost nebo rozhodnutí podle odstavců 2, 3 a 4 případně odvolal. Příslušný orgán vydá v přiměřené lhůtě po obdržení žádosti poskytovatele hostingových služeb odůvodněné rozhodnutí.

Článek 7

Uchovávání obsahu a souvisejících údajů

1. Poskytovatelé hostingových služeb uchovávají teroristický obsah, který byl odstraněn nebo k němuž byl znemožněn přístup v důsledku příkazu k odstranění, hlášení či proaktivních opatření podle článků 4, 5 a 6, jakož i související údaje, jež byly odstraněny v důsledku odstranění teroristického obsahu**,** […] jež jsou nutné pro účely:

   a) správního nebo soudního přezkumu;

   b) prevence, odhalování, vyšetřování či stíhání teroristických trestných činů.

2. Teroristický obsah a související údaje uvedené v odstavci 1 se uchovávají po dobu šesti měsíců. Teroristický obsah se na žádost příslušného orgánu nebo soudu uchovává po dobu delší, pokud a dokud je to nezbytné pro účely probíhajícího správního nebo soudního přezkumu uvedeného v odst. 1 písm. a).

3. Poskytovatelé hostingových služeb zajistí, aby byl teroristický obsah a související údaje uchovávané podle odstavců 1 a 2 předmětem vhodných technických a organizačních záruk.

   Tyto technické a organizační záruky zajistí, aby byly uchovaný teroristický obsah a související údaje zpřístupněny a zpracovány pouze pro účely uvedené v odstavci 1 a aby byla zajištěna vysoká úroveň bezpečnosti dotčených osobních údajů. Poskytovatelé hostingových služeb tyto záruky v případě potřeby přezkoumají a aktualizují.

ODDÍL III
ZÁRUKY A ODPOVĚDNOST

Článek 8

Povinnosti týkající se transparentnosti

1. Poskytovatelé hostingových služeb vymezí ve svých podmínkách svou politiku týkající se prevence šíření teroristického obsahu, včetně případného smysluplného vysvětlení fungování aktivních opatření, včetně používání automatizovaných nástrojů.

2. Poskytovatelé hostingových služeb […] ***vystavení teroristickému obsahu*** zveřejňují výroční zprávy o transparentnosti, pokud jde o opatření přijatá proti šíření teroristického obsahu.

3. Zprávy o transparentnosti musejí obsahovat alespoň tyto údaje:

   a) informace o opatřeních poskytovatele hostingových služeb v souvislosti s odhalováním, identifikací a odstraňováním teroristického obsahu;

   b) informace o opatřeních poskytovatele hostingových služeb […] ***pro účinné řešení*** opětovného […] ***výskytu*** obsahu, který byl již dříve odstraněn nebo k němuž byl znemožněn přístup, protože je považován za teroristický;

   c) počet položek teroristického obsahu, který byl odstraněn nebo k němuž byl znemožněn přístup na základě příkazů k odstranění, hlášení či případně proaktivních opatření;

   d) přehled a výsledky řízení o stížnostech.

Článek 9

Záruky týkající se používání a zavádění proaktivních opatření

1. Jestliže poskytovatelé hostingových služeb zpracovávají obsah, který uchovávají, automatizovanými nástroji podle tohoto nařízení, poskytnou efektivní a vhodné záruky, které zajistí, že rozhodnutí o daném obsahu, zejména rozhodnutí o odstranění obsahu nebo znemožnění přístupu k obsahu považovanému za teroristický, jsou přesná a odůvodněná.

2. Záruky sestávají zejména z lidského dohledu a kontroly v případě potřeby a v každém případě tehdy, pokud je podrobné posouzení příslušného kontextu nutné k tomu, aby se stanovilo, má-li se obsah považovat za teroristický.

Článek 10

Mechanismy pro podávání stížností

1. Poskytovatelé hostingových služeb zavedou účinné a přístupné mechanismy, které poskytovatelům obsahu, jejichž obsah byl odstraněn nebo k němuž byl znemožněn přístup na základě hlášení podle článku 5 nebo proaktivních opatření podle článku 6, umožňují podat stížnost proti zásahu poskytovatele hostingových služeb s žádostí o obnovení obsahu.

2. Poskytovatelé hostingových služeb neprodleně prošetří všechny stížnosti, které obdrží, a bez zbytečného prodlení obsah obnoví v případech, kdy je jeho odstranění či znemožnění přístupu k němu neoprávněné. O výsledku šetření informují stěžovatele.

Článek 11

Informace pro poskytovatele obsahu

1. Jestliže poskytovatelé hostingových služeb teroristický obsah odstraní nebo k němu znemožní přístup, informace o odstranění teroristického obsahu či znemožnění přístupu k němu zpřístupní poskytovateli obsahu.

2. Poskytovatel hostingových služeb poskytovatele obsahu na jeho žádost informuje o důvodech pro odstranění či znemožnění přístupu, jakož i o možnostech napadení tohoto rozhodnutí.

3. Povinnost podle odstavců 1 a 2 se nevztahuje na případy, kdy příslušný orgán rozhodne, že by z důvodu veřejné bezpečnosti, jako je prevence, vyšetřování, odhalování a stíhání teroristických trestných činů, neměly být zveřejněny žádné informace, a to po dobu nezbytně nutnou, avšak […] ne delší než […] ***šest*** týdnů od uvedeného rozhodnutí. ***Tato lhůta může být v odůvodněných případech jednou prodloužena o dalších šest týdnů.*** V takovém případě poskytovatel hostingových služeb nezveřejní žádné informace o odstranění teroristického obsahu nebo znemožnění přístupu k němu.

ODDÍL IV

Spolupráce mezi příslušnými orgány, subjekty Unie a poskytovateli hostingových služeb

Článek 12

Kapacita příslušných orgánů

Členské státy zajistí, aby jejich příslušné orgány měly nezbytnou kapacitu a dostatečné zdroje k dosažení cílů a plnění svých povinností vyplývajících z tohoto nařízení.

Článek 13

*Spolupráce mezi poskytovateli hostingových služeb, příslušnými orgány a případně […] **příslušnými** subjekty Unie*

1. Příslušné orgány v členských státech se ve věci příkazů k odstranění a hlášení navzájem informují, koordinují svoji činnost, spolupracují mezi sebou a případně také s […] ***příslušnými*** subjekty Unie, jako je Europol, aby se zabránilo duplicitě, posílila se koordinace a zabránilo se zásahům do šetření v jiných členských státech.

2. Příslušné orgány v členských státech informují příslušný orgán uvedený v čl. 17 odst. 1 písm. c) a d), koordinují činnost s tímto orgánem a spolupracují s ním, pokud jde o opatření přijatá podle článku 6 a donucovací opatření podle článku 18. Členské státy zajistí, aby měl příslušný orgán uvedený v čl. 17 odst. 1 písm. c) a d) k dispozici veškeré relevantní informace. Za tímto účelem členské státy zajistí vhodné komunikační kanály nebo mechanismy, aby byly příslušné informace sdíleny včas.

3. ***Pro účinné provádění tohoto nařízení a zabránění duplicitě se č***lenské státy a poskytovatelé hostingových služeb mohou rozhodnout, že využijí specializované nástroje, případně včetně [...] nástrojů zavedených [...] ***příslušnými*** subjekty Unie, jako je Europol, a to zejména za účelem usnadnění:

a) zpracování a zpětné vazby, jež se týkají příkazů k odstranění podle článku 4;

b) zpracování a zpětné vazby, jež se týkají hlášení podle článku 5;

c) spolupráce, jejímž cílem je vymezit a provádět proaktivní opatření podle článku 6.

4. Pokud se poskytovatelé hostingových služeb dozvědí o jakémkoli důkazu teroristických trestných činů, neprodleně uvědomí orgány odpovědné za vyšetřování a stíhání trestných činů v [...] dotyčném členském státě ***nebo státech*** [...]. ***Není-li možno dotyčný členský stát nebo státy identifikovat,*** [...] poskytovatelé hostingových služeb [...] ***uvědomí kontaktní místo podle čl. 14 odst. 3 v členském státě, kde mají svou hlavní provozovnu nebo právního zástupce, a*** postoupí dané informace rovněž Europolu za účelem provedení příslušných následných opatření.

Článek 14

Kontaktní místa

1. Poskytovatelé hostingových služeb zřídí kontaktní místo umožňující příjem příkazů k odstranění a hlášení elektronickou cestou a zajistí jejich rychlé zpracování podle článků 4 a 5. Zajistí, aby tyto informace byly veřejně dostupné.

2. V informacích zmíněných v odstavci 1 musí být upřesněn úřední jazyk nebo jazyky Unie, jak jsou uvedeny v nařízení č. 1/58, v nichž je možné se obrátit na kontaktní místo a ve kterých se uskuteční další výměny informací o příkazech k odstranění a hlášeních podle článků 4 a 5. To zahrnuje alespoň jeden z úředních jazyků členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má bydliště nebo je usazen jeho právní zástupce podle článku 16.

3. Členské státy zřídí kontaktní místo pro vyřizování žádostí o objasnění a zpětnou vazbu týkající se příkazů k odstranění a hlášení jimi vydaných. Informace o kontaktním místě jsou veřejně dostupné.

ODDÍL V
PROVÁDĚNÍ A PROSAZOVÁNÍ

Článek 15

Příslušnost

1. Členský stát, v němž se nachází hlavní provozovna poskytovatele hostingových služeb, je příslušný pro účely článků 6, 18 a 21. Poskytovatel hostingových služeb, jehož hlavní provozovna není v některém z členských států, se považuje za poskytovatele hostingových služeb, který spadá do příslušnosti členského státu, v němž má bydliště nebo je usazen právní zástupce uvedený v článku 16. ***Členský stát má příslušnost pro účely článků 4 a 5 bez ohledu na to, kde má poskytovatel služeb své hlavní sídlo nebo kde určil právního zástupce.***

2. Pokud poskytovatel hostingových služeb nejmenuje právního zástupce, jsou příslušné všechny členské státy. ***Pokud se členský stát rozhodne vykonávat svou příslušnost, uvědomí o tom všechny ostatní členské státy.***

[…] […]

Článek 16

Právní zástupce

1. Poskytovatel hostingových služeb, který nemá provozovnu v Unii, ale nabízí v Unii služby, určí písemně právnickou nebo fyzickou osobu, která je jeho právním zástupcem v Unii pro příjem, dodržování a výkon příkazů k odstranění, hlášení, žádostí a rozhodnutí vydaných příslušnými orgány na základě tohoto nařízení. Právní zástupce má bydliště nebo je usazen v jednom z členských států, v nichž poskytovatel hostingových služeb nabízí služby.

2. Poskytovatel hostingových služeb svěří právnímu zástupci přijetí, dodržování a výkon příkazů k odstranění, hlášení, žádostí a rozhodnutí uvedených v odstavci 1 jménem dotčeného poskytovatele hostingových služeb. Poskytovatelé hostingových služeb poskytnou svému právnímu zástupci nezbytné pravomoci a zdroje ke spolupráci s příslušnými orgány a k plnění těchto rozhodnutí a příkazů.

3. Určený právní zástupce může nést odpovědnost za nedodržení povinností vyplývajících z tohoto nařízení, aniž je tím dotčena odpovědnost poskytovatele hostingových služeb a právní opatření, která by proti němu mohla být zahájena.

4. Poskytovatel hostingových služeb o určení informuje příslušný orgán uvedený v čl. 17 odst. 1 písm. d) v členském státě, ve kterém má bydliště nebo v němž je usazen právní zástupce. Informace o právním zástupci jsou veřejně dostupné.

ODDÍL VI
ZÁVĚREČNÁ USTANOVENÍ

Článek 17

Určení příslušných orgánů

1. Každý členský stát určí příslušný orgán nebo orgány k:

   a) vydávání příkazů k odstranění podle článku 4.

   b) odhalování, identifikaci a hlášení teroristického obsahu poskytovatelům hostingových služeb podle článku 5;

   c) dohledu na provádění proaktivních opatření podle článku 6;

   d) výkonu povinnosti podle tohoto nařízení prostřednictvím sankcí podle článku 18.

2. Členský stát oznámí Komisi příslušný ***orgán nebo*** orgány uvedené v odstavci 1 nejpozději do [***dvanácti*** […] *měsíců od vstupu tohoto nařízení v platnost*]. Komise toto hlášení a veškeré jeho změny zveřejní v *Úředním věstníku Evropské unie*.

Článek 18

Sankce

1. Členské státy stanoví pravidla pro sankce za porušení povinností ze strany poskytovatelů hostingových služeb podle tohoto nařízení a přijmou veškerá opatření nezbytná pro jejich provedení. Tyto sankce se omezují na porušení povinností vyplývajících z:

   a) čl. 3 odst. 2 (podmínky poskytovatelů hostingových služeb);

   b) čl. 4 odst. 2 a 6 (provádění a zpětná vazba týkající se příkazů k odstranění);

c) čl. 5 odst. 5 a 6 (posouzení a zpětná vazba týkající se hlášení);

d) čl. 6 odst. 2 a 4 (zprávy o proaktivních opatřeních a přijetí opatření na základě rozhodnutí o uložení zvláštních proaktivních opatření);

e) článku 7 (uchovávání údajů);

f) článku 8 (transparentnost);

g) článku 9 (záruky týkající se proaktivních opatření);

h) článku 10 (postupy pro podávání stížností);

i) článku 11 (informace pro poskytovatele obsahu)

j) čl. 13 odst. 4 (informace o důkazu teroristických trestných činů);

k) čl. 14 odst. 1 (kontaktní místa);

l) článku 16 (určení právního zástupce).

2. Stanovené sankce musí být účinné, přiměřené a odrazující. Členské státy nejpozději do [*během měsíců od vstupu tohoto nařízení v platnost*] oznámí Komisi tato pravidla a tato opatření a budou ji neprodleně informovat o všech následných změnách, které se jich budou týkat.

3. Členské státy zajistí, aby příslušné orgány při určování druhu a výše sankcí zohledňovaly všechny relevantní okolnosti, včetně:

a) povahy, závažnosti a doby trvání porušení;

b) záměrné či nedbalostní povahy porušení;

c) předchozích porušení předpisů odpovědnou právnickou ***nebo fyzickou*** osobou;

d) finanční síly odpovědné právnické ***nebo fyzické*** osoby;

e) úrovně spolupráce poskytovatele hostingových služeb s příslušnými orgány.

4. Členské státy zajistí, aby systematické nedodržování povinností podle čl. 4 odst. 2 podléhalo finančním sankcím ve výši až 4 % celosvětového obratu poskytovatele hostingových služeb v posledním hospodářském roce.

Článek 19

Technické požadavky a změny šablon příkazů k odstranění

1. Komisi se svěřuje pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 20 za účelem doplnění tohoto nařízení o technické požadavky na elektronické prostředky, které mají příslušné orgány používat při předávání příkazů k odstranění.

2. Komise se zmocňuje k přijímání takových aktů v přenesené pravomoci za účelem změn přílohy I, II a III, aby účinně řešila případnou potřebu zlepšení obsahu formulářů příkazu k odstranění a formulářů používaných k poskytnutí informací o nemožnosti provést příkaz k odstranění.

Článek 20

Výkon přenesené pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v článku 19 je svěřena Komisi na dobu neurčitou počínaje [*datum vstupu tohoto nařízení v platnost*].

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v článku 19 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm blíže určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v Úředním věstníku Evropské unie, nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Před přijetím aktu v přenesené pravomoci Komise vede konzultace s odborníky určenými jednotlivými členskými státy v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů.

5. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

6. Akt v přenesené pravomoci přijatý podle článku 19 vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

Článek 21

Sledování

1. Členské státy shromažďují od svých příslušných orgánů a poskytovatelů hostingových služeb, kteří spadají do jejich pravomoci, informace o opatřeních, která přijaly v souladu s tímto nařízením, a tyto informace každoročně do [31. března] zasílají Komisi. Uvedené informace musí zahrnovat:

   a) informace o počtu vydaných příkazů k odstranění a vydaných hlášení, o počtu položek teroristického obsahu, které byly odstraněny nebo k nimž byl znemožněn přístup, včetně uvedení příslušných časových lhůt podle článků 4 a 5;

b) informace o zvláštních proaktivních opatřeních přijatých podle článku 6, včetně množství teroristického obsahu, který byl odstraněn nebo k němuž byl znemožněn přístup a příslušných časových lhůt;

c) informace o počtu zahájených postupů pro podávání stížností a o opatřeních přijatých poskytovateli hostingových služeb podle článku 10;

d) informace o počtu zahájených odvolacích řízeních a o rozhodnutích přijatých příslušným orgánem v souladu s vnitrostátními právními předpisy.

2. Nejpozději do [*jeden rok od data použitelnosti tohoto nařízení*] zavede Komise podrobný program monitorování výstupů, výsledků a dopadů tohoto nařízení. Program monitorování stanoví ukazatele, prostředky a intervaly shromažďování údajů a dalších potřebných důkazů. Stanoví opatření, která má Komise a členské státy přijmout při shromažďování a analýze údajů a jiných důkazů za účelem monitorování výsledků a hodnocení tohoto nařízení podle článku 23.

Článek 22

Zpráva o provádění

Do... [*dva roky po vstupu tohoto nařízení v platnost*] předloží Komise Evropskému parlamentu a Radě zprávu o uplatňování tohoto nařízení. Ve zprávě Komise se zohlední informace o monitorování podle článku 21 a informace vyplývající z povinností týkajících se transparentnosti podle článku 8. Členské státy poskytnou Komisi informace, které jsou pro vypracování zprávy nezbytné.

Článek 23

Hodnocení

Nejdříve [*tři roky ode dne použitelnosti tohoto nařízení*] provede Komise hodnocení tohoto nařízení a předloží Evropskému parlamentu a Radě zprávu o jeho uplatňování, včetně fungování účinnosti ochranných mechanismů. V případě potřeby ke zprávě připojí legislativní návrhy. Členské státy poskytnou Komisi informace, které jsou pro vypracování zprávy nezbytné.

Článek 24

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Použije se od [***12*** […] měsíců po vstupu v platnost].

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne

Za Evropský parlament	*Za Radu*
předseda	*předseda nebo předsedkyně*