NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2021/784

ze dne 29. dubna 2021

o potírání šíření teroristického obsahu online

(Text s významem pro EHP)

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 výboru ([1]),

v souladu s řádným legislativním postupem ([2]),

vzhledem k těmto důvodům:

(1) Cílem tohoto nařízení je zajistit řádné fungování jednotného digitálního trhu v otevřené a demokratické společnosti tím, že se zaměřuje na boj proti zneužívání hostingových služeb pro teroristické účely a přispívá k veřejné bezpečnosti v celé Unii. V zájmu lepšího fungování jednotného digitálního trhu je třeba zvyšovat právní jistotu poskytovatelů hostingových služeb a důvěru uživatelů v internetové prostředí, jakož i posilovat záruky svobody projevu, včetně svobody přijímat a rozšiřovat informace a myšlenky v otevřené a demokratické společnosti, a svobody a plurality sdělovacích prostředků.

(2) Regulační opatření zaměřená na potírání šíření teroristického obsahu online by měly doplňovat strategie členských států zaměřené na boj proti terorismu, zahrnující posilování mediální gramotnosti a kritického myšlení, vytváření alternativní argumentace a protiargumentace, a další iniciativy ke snížení dopadu teroristického obsahu online a zvýšení odolnosti vůči němu, jakož i investice do sociální práce, iniciativ zaměřených na deradikalizaci a spolupráce s dotčenými komunitami s cílem dosáhnout trvalé prevence radikalizace ve společnosti.

(3) Potírání teroristickému obsahu online, který je součástí širšího problému nezákonného obsahu online, vyžaduje kombinaci legislativních, nelegislativních a dobrovolných opatření založených na spolupráci mezi orgány a poskytovateli hostingových služeb při plném dodržování základních práv.

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

([1]) Úř. věst. C 110, 22.3.2019, s. 67.

([2]) Postoj Evropského parlamentu ze dne 17. dubna 2019 (dosud nezveřejněný v Úředním věstníku) a postoj Rady v prvním čtení ze dne 16. března 2021 (Úř. věst. C 135, 16.4.2021, s. 1). Postoj Evropského parlamentu ze dne 28. dubna 2021 (dosud nezveřejněný v Úředním věstníku).

(5) Ačkoli přítomnost teroristického obsahu online není jediným faktorem, ukázala se být katalyzátorem radikalizace jednotlivců, jež může vést k teroristickým činům, a má proto 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 k poškozování jejich obchodních modelů. Vzhledem k tomu, že poskytovatelé hostingových služeb zastávají ústřední úlohu a mají k dispozici technologické prostředky a kapacity související s poskytovanými službami, mají ve vztahu ke společnosti zvláštní odpovědnost chránit své poskytované služby před zneužitím teroristy a účastnit se potírání teroristického obsahu, který je prostřednictvím jejich služeb online šířen, přičemž musejí zohlednit zásadní význam svobody projevu, včetně svobody přijímat a rozšiřovat informace a myšlenky v otevřené a demokratické společnosti.

(6) Úsilí v potírání teroristického obsahu online bylo na úrovni Unie započato v roce 2015 v rámci dobrovolné spolupráce mezi členskými státy a poskytovateli hostingových služeb. Má-li být dostupnost teroristického obsahu online dále snižována a má-li být tento rychle narůstající problém náležitě vyřešen, je třeba toto úsilí doplnit o jasný legislativní rámec. Tento legislativní rámec navazuje na dobrovolné úsilí, které bylo podpořeno doporučením Komise (EU) 2018/334 ([3]), a reaguje na výzvy Evropského parlamentu, aby byla posílena opatření zaměřená na boj proti nezákonnému a škodlivému obsahu online, v souladu s horizontálním rámcem zavedeným směrnicí Evropského parlamentu a Rady 2000/31/ES ([4]) a Evropskou radou, v zájmu účinnějšího identifikování a odstraňování obsahu online, jenž podněcuje k teroristickým činům.

(7) Tímto nařízením by nemělo být dotčeno uplatňování směrnice 2000/31/ES. Především by pak opatření přijatá poskytovatelem hostingových služeb v souladu s tímto nařízením, a to včetně jakýchkoli zvláštních opatření, neměla sama o sobě vést k tomu, že se na poskytovatele hostingových služeb přestane vztahovat výjimka z odpovědnosti stanovená uvedenou směrnicí. Tímto nařízením nejsou dotčeny pravomoci vnitrostátních orgánů a soudů stanovit odpovědnost poskytovatelů hostingových služeb v případech, kdy nejsou splněny podmínky pro výjimku z odpovědnosti podle uvedené směrnice.

(8) V případě rozporu mezi tímto nařízením a směrnicí Evropského parlamentu a Rady 2010/13/EU ([5]), pokud jde o ustanovení upravující audiovizuální mediální služby ve smyslu čl. 1 odst. 1 písm. a) uvedené směrnice, by měla mít přednost směrnice 2010/13/EU. Tím by neměly být dotčeny povinnosti podle tohoto nařízení, a to zejména pokud jde o poskytovatele platforem pro sdílení videonahrávek.

(9) Toto nařízení by mělo stanovit pravidla týkající se boje proti zneužívání hostingových služeb k šíření teroristického obsahu online, jež mají zaručit hladké fungování vnitřního trhu. Tato pravidla by měla plně respektovat základní práva chráněná v Unii, a zejména práva zaručená Listinou základních práv Evropské unie (dále jen „Listina“).

(10) Účelem tohoto nařízení je přispět k ochraně veřejné bezpečnosti a současně stanovit náležité a účinné záruky k zajištění ochrany základních práv včetně práva na respektování soukromého života, práva na ochranu osobních údajů, práva na svobodu projevu, a to včetně práva přijímat a rozšiřovat informace, práva na svobodu podnikání a práva na účinnou právní ochranu. Rovněž je zakázána jakákoliv diskriminace. Příslušné orgány a poskytovatelé hostingových služeb by měli přijímat pouze opatření, která jsou nutná, vhodná a přiměřená v demokratické společnosti, a to s ohledem na zvláštní význam svobody projevu a informací a svobody a plurality sdělovacích prostředků, které představují základní pilíře pluralitní a demokratické společnosti a zároveň jsou hodnotami, na kterých je Unie založena. Opatření, která se týkají svobody projevu a informací, by měla být cíleně zaměřená, aby sloužila k potírání šíření teroristického obsahu online, avšak zároveň ctila právo legálně přijímat a rozšiřovat informace, a přitom zohledňovala ústřední úlohu, kterou poskytovatelé hostingových služeb zastávají při zprostředkování veřejné diskuse a šíření a přijímání faktů, názorů a myšlenek v souladu se zákonem. Účinná opatření online proti teroristickému obsahu online a ochrana svobody projevu a informací nejsou protichůdnými cíli, nýbrž cíli, které se vzájemně doplňují a posilují.

([3]) 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, s. 50).

([4]) 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).

([5]) Směrnice Evropského parlamentu a Rady 2010/13/EU ze dne 10. března 2010 o koordinaci některých právních a správních předpisů členských států upravujících poskytování audiovizuálních mediálních služeb (směrnice o audiovizuálních mediálních službách) (Úř. věst. Úř. věst. L 95, 15.4.2010, s. 1).

(11) Aby se vyjasnilo, jaká opatření mají poskytovatelé hostingových služeb a příslušné orgány přijmout proti šíření teroristického obsahu online, mělo by toto nařízení stanovit definici „teroristického obsahu" pro preventivní účely, která bude v souladu s definicemi příslušných trestných činů stanovenými ve směrnici Evropského parlamentu a Rady (EU) 2017/541 ([6]). Jelikož je třeba bojovat proti nejškodlivější teroristické propagandě online, měla by tato definice zahrnovat materiál, který podněcuje nebo získává jiné osoby ke spáchání nebo přispění ke spáchání teroristických trestných činů, získává jiné osoby k účasti na činnostech teroristické skupiny nebo glorifikuje teroristické činnosti, mimo jiné i šířením materiálu zobrazujícího teroristický útok. Tato definice by měla rovněž zahrnovat materiál, který poskytuje návod k výrobě nebo použití výbušnin, palných nebo jiných zbraní nebo škodlivých či nebezpečných látek, jakož i chemických, biologických, radiologických a jaderných (CBRN) látek, nebo k jiným specifickým metodám či technikám, včetně výběru cílů, za účelem spáchání nebo přispění ke spáchání teroristických trestných činů. Takový materiál zahrnuje text, obrazy, zvukové nahrávky a videa, jakož i živý přenos teroristických trestných činů, jež vyvolávají nebezpečí, že mohou být spáchány další takové trestné činy. Při posuzování, zda je materiál teroristickým obsahem ve smyslu tohoto nařízení, by příslušné orgány a poskytovatelé hostingových služeb měli zohlednit faktory, jakými jsou povaha a znění výroků či projevů, kontext, ve kterém byly učiněny, a jejich potenciál přivodit škodlivé důsledky, pokud jde o bezpečnost a ochranu osob. Skutečnost, že byl materiál vytvořen osobou, skupinou či subjektem zařazenými na unijní seznam osob, skupin a subjektů zapojených do teroristických trestných činů, na které se vztahují omezující opatření, lze jej osobě, skupině nebo subjektu přičítat nebo je šířen jejich jménem, by mělo být při posouzení důležitým faktorem.

(12) Za teroristický obsah by neměl být považován materiál šířený pro vzdělávací, žurnalistické, umělecké nebo výzkumné účely nebo pro osvětové účely namířené proti teroristické činnosti. Při určování toho, zda je materiál poskytnutý poskytovatelem obsahu „teroristickým obsahem" ve smyslu tohoto nařízení, by mělo být zohledněno zejména právo na svobodu projevu a informací, včetně svobody a plurality sdělovacích prostředků, a svoboda umění a věd. Zejména v případech, kdy poskytovatel obsahu nese redakční odpovědnost, by každé rozhodnutí týkající se odstranění šířeného materiálu mělo zohledňovat standardy novinářské práce stanovené v předpisech upravujících oblast tisku nebo sdělovacích prostředků v souladu s právem Unie včetně Listiny. Navíc by nemělo být za teroristický obsah považováno vyjadřování radikálních, polemických či kontroverzních názorů ve veřejné diskuzi o citlivých politických otázkách.

(13) V zájmu účinného potírání šíření teroristického obsahu online a zároveň v zájmu zajištění respektování soukromého života jednotlivců by se toto nařízení mělo vztahovat na poskytovatele služeb informační společnosti, kteří na žádost uživatele služby uchovávají a veřejně šíří jím poskytnutý materiál nebo informace, bez ohledu na to, zda je uchovávání a veřejné šíření těchto informací a materiálu pouze technické, automatické nebo pasivní povahy. Pojmem „uchovávání" by se mělo rozumět držení dat uložených v paměti fyzického nebo virtuálního serveru. Poskytovatelé služeb „prostého přenosu" a služeb ukládání do vyrovnávací paměti (tzv. „caching"), jakož i jiných služeb poskytovaných v jiných vrstvách internetové infrastruktury, které uchovávání nezahrnují, jako jsou registry a registrátoři, poskytovatelé systémů doménových jmen (DNS), platební služby nebo služby ochrany před distribuovaným odepřením služby (DDoS), by proto do oblasti působnosti tohoto nařízení spadat neměli.

(14) Pojem „veřejné šíření" by měl zahrnovat zpřístupňování informací potenciálně neomezenému počtu osob, kdy je uživatelům obecně umožněn snadný přístup k informacím, aniž by byl ze strany poskytovatele obsahu požadován jakýkoliv další krok, a to bez ohledu na to, zda tyto osoby přístup k daným informacím skutečně využijí. Proto pokud přístup k informacím vyžaduje registraci nebo přijetí do určité skupiny uživatelů, měly by se tyto informace považovat za veřejně šířené pouze v případě, že k registraci uživatelů usilujících o přístup k informacím nebo k jejich přijetí do skupiny dochází automaticky, aniž by proběhlo lidské rozhodnutí nebo výběr osob, jimž se přístup udělí. Do oblasti působnosti tohoto nařízení by neměly spadat interpersonální komunikační služby ve smyslu čl. 2 bodu 5 směrnice Evropského parlamentu a Rady (EU) 2018/1972 ([7]), jako jsou e-maily nebo služby zasílání soukromých zpráv. Informace by měly být považovány za uchovávané a veřejně šířené ve smyslu tohoto

([6]) 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).

([7]) Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace (Úř. věst. L 321, 17.12.2018, s. 36).

nařízení, pouze pokud jsou tyto činnosti vykonávány na základě přímé žádosti poskytovatele obsahu. Proto by se toto nařízení nemělo vztahovat na poskytovatele služeb, jako je cloudová infrastruktura, které jsou poskytovány na žádost jiných stran než poskytovatelů obsahu a ze kterých mají poskytovatelé obsahu pouze nepřímý prospěch. Toto nařízení by se mělo vztahovat například na poskytovatele služeb sociálních médií, služeb sdílení videa, obrazového a zvukového materiálu, jakož i služeb sdílení souborů a jiných cloudových služeb, pokud jsou tyto služby využívány k veřejnému zpřístupnění uchovávaných informací na přímou žádost poskytovatele obsahu. Pokud poskytovatel hostingových služeb nabízí více služeb, mělo by se toto nařízení vztahovat pouze na služby, které spadají do jeho oblasti působnosti.

(15) Teroristický obsah je často veřejně šířen prostřednictvím služeb poskytovaných poskytovateli hostingových služeb usazenými ve třetích zemích. Aby byli uživatelé v Unii chráněni a aby bylo zajištěno, že se na všechny poskytovatele hostingových služeb působící na jednotném digitálním trhu vztahují stejné požadavky, mělo by se toto nařízení použít na všechny poskytovatele příslušných služeb nabízených v Unii bez ohledu na zemi, kde mají hlavní provozovnu. Mělo by se mít za to, že poskytovatel hostingových služeb nabízí služby v Unii, pokud umožňuje fyzickým nebo právnickým osobám v jednom či více členských státech využívat své služby a má-li s tímto členským státem nebo s těmito členskými státy podstatné spojení.

(16) Podstatné spojení s Unií by mělo existovat, pokud má poskytovatel hostingových služeb provozovnu v Unii, jeho služeb využívá významný počet uživatelů v jednom nebo více členských státech nebo jsou jeho činnosti zaměřeny na jeden nebo více členských států. Zaměření činností na jeden nebo více členských států by mělo být určeno na základě všech relevantních okolností, včetně takových faktorů, jako je používání jazyka či měny obecně používaných v dotyčném členském státě nebo možnost objednání zboží či služeb z tohoto členského státu. Uvedené zaměření by mohlo být též odvozeno od dostupnosti aplikace v obchodě s aplikacemi příslušného členského státu, od používání místních reklam nebo reklam v jazyce obecně používaném v dotyčném členském státě nebo od řešení vztahů se zákazníky, jako je poskytování zákaznického servisu v jazyce obecně používaném v tomto členském státě. Podstatné spojení by mělo být předpokládáno i v případě, že poskytovatel hostingových služeb zaměřuje svoje činnosti na jeden nebo více členských států, jak stanoví čl. 17 odst. 1 písm. c) nařízení Evropského parlamentu a Rady (EU) č. 1215/2012 ([8]). Pouhá dostupnost internetové stránky, e-mailové adresy nebo jiných kontaktních údajů poskytovatele hostingových služeb v jednom nebo více členských státech by sama o sobě neměla být dostatečná k tomu, aby zakládala podstatné spojení. Kromě toho by poskytování služby s cílem pouhého souladu se zákazem diskriminace, jak jej stanoví nařízení Evropského parlamentu a Rady (EU) 2018/302 ([9]), nemělo být považováno za to, že zakládá podstatné spojení s Unií.

(17) Je třeba harmonizovat postup a povinnosti vyplývající z příkazů k odstranění, kterými se po posouzení příslušnými orgány poskytovatelům hostingových služeb ukládá, aby odstranili teroristický obsah nebo znemožnili přístup k němu. S ohledem na rychlost šíření teroristického obsahu napříč online službami by měla být poskytovatelům hostingových služeb uložena povinnost zajistit, aby byl teroristický obsah určený v příkazu k odstranění odstraněn nebo přístup k němu znemožněn ve všech členských státech do jedné hodiny od přijetí příkazu k odstranění. Vyjma řádně odůvodněných naléhavých případů by měl příslušný orgán poskytnout poskytovateli hostingových služeb informace o postupech a platných lhůtách alespoň dvanáct hodin před vydáním prvního příkazu k odstranění vůči tomuto poskytovateli hostingových služeb. Takovéto řádně odůvodněné naléhavé případy nastanou, pokud by odstranění teroristického obsahu nebo znemožnění přístupu k němu později než jednu hodinu od obdržení příkazu k odstranění způsobilo vážnou újmu, například v situacích bezprostředního ohrožení života nebo fyzické integrity osoby, nebo pokud by tento obsah zobrazoval právě probíhající události, které působí újmu na životě nebo fyzické integritě osoby. Příslušný orgán by měl určit, zda se jedná o naléhavý případ, a své rozhodnutí v příkazu k odstranění řádně odůvodnit. Pokud poskytovatel hostingových služeb nemůže příkaz k odstranění splnit do jedné hodiny od jeho přijetí z důvodu vyšší moci nebo faktické nemožnosti, včetně objektivně opodstatněných technických nebo provozních důvodů, měl by o tom co nejdříve informovat vydávající příslušný orgán a příkaz k odstranění splnit, jakmile se situace vyřeší.

([8]) 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, s. 1).

([9]) 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 60 I, 2.3.2018, s. 1).

(18) Příkaz k odstranění by měl obsahovat odůvodnění pro označení materiálu, který má být odstraněn nebo k němuž má být znemožněn přístup, za teroristický obsah a poskytovat informace dostatečné pro lokalizaci tohoto obsahu s uvedením přesné adresy URL a v případě potřeby veškerých dalších doplňujících informací, jako je například snímek obrazovky zachycující daný obsah. Odůvodnění by mělo poskytovateli hostingových služeb a v konečném důsledku i poskytovateli obsahu umožnit účinně vykonat své právo na soudní nápravu. Poskytnutí odůvodnění by nemělo zahrnovat zveřejnění citlivých informací, které by mohly ohrozit probíhající vyšetřování.

(19) Příslušný orgán by měl příkaz k odstranění předložit přímo kontaktnímu místu určenému nebo zřízenému poskytovatelem hostingových služeb pro účely tohoto nařízení elektronickými prostředky umožňujícími vytvoření písemného záznamu za podmínek, jež poskytovateli hostingových služeb umožňují ověřit pravost příkazu, včetně přesnosti data a času odeslání a přijetí příkazu, například zabezpečenou e-mailovou poštou nebo platformou nebo jinými zabezpečenými kanály, včetně těch, které dá k dispozici poskytovatel hostingových služeb, a to v souladu s právními předpisy Unie na ochranu osobních údajů. Tento požadavek by mělo být možné splnit například s využitím kvalifikovaných služeb elektronického doporučeného doručování, jak stanoví nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ([10]). Má-li poskytovatel hostingových služeb hlavní provozovnu nebo právního zástupce s bydlištěm nebo usazeného v jiném členském státě, než je členský stát vydávajícího příslušného orgánu, měla by být kopie příkazu k odstranění současně zaslána příslušnému orgánu tohoto členského státu.

(20) Příslušný orgán členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má jeho právní zástupce bydliště nebo je usazen, by měl mít možnost příkaz k odstranění vydaný příslušnými orgány jiného členského státu přezkoumat s cílem určit, zda závažně nebo zjevně neporušuje toto nařízení nebo základní práva zakotvená v Listině. Poskytovatel obsahu i poskytovatel hostingových služeb by měli mít právo požádat o takový přezkum příslušným orgánem v členském státě, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má jeho právní zástupce bydliště nebo je usazen. Pokud je taková žádost podána, měl by daný příslušný orgán přijmout rozhodnutí, zda u příkazu k odstranění došlo k takovým porušením. Pokud uvedené rozhodnutí taková porušení konstatuje, měl by příkaz k odstranění pozbýt právních účinků. Přezkum by měl být proveden urychleně, aby bylo zajištěno co nejrychlejší obnovení chybně odstraněného obsahu nebo obsahu, ke kterému byl znemožněn přístup.

(21) Poskytovatelé hostingových služeb vystavení teroristickému obsahu by měli do svých podmínek, pokud je stanovili, zařadit ustanovení týkající se boje proti zneužívání jejich služeb k veřejnému šíření teroristického obsahu. Měli by tato ustanovení uplatňovat s řádnou péčí, transparentně, přiměřeně a nediskriminačně.

(22) S ohledem na rozsah problému a rychlost, jíž je k efektivnímu identifikování a odstraňování teroristického obsahu zapotřebí, představují zásadní prvek v potírání šíření teroristickému obsahu online účinná a přiměřená zvláštní opatření. Poskytovatelé hostingových služeb vystavení teroristickému obsahu by měli za účelem omezení dostupnosti teroristického obsahu v rámci svých služeb zavést zvláštní opatření, přičemž by měli zohlednit rizika a míru vystavení teroristickému obsahu, jakož i dopady na práva třetích stran a informace ve veřejném zájmu. Poskytovatelé hostingových služeb by měli určit, jaká vhodná, účinná a přiměřená zvláštní opatření by měla být zavedena s cílem identifikovat a odstraňovat teroristický obsah. Zvláštní opatření by mohla zahrnovat vhodná technická nebo provozní opatření nebo kapacity, jako například personální obsazení nebo technické prostředky pro identifikaci a rychlé odstranění teroristického obsahu nebo znemožnění přístupu k němu, mechanismy umožňující uživatelům oznamovat nebo označovat domnělý teroristický obsah nebo jakákoli jiná opatření, která poskytovatel hostingových služeb považuje za vhodná a účinná pro řešení problému dostupnosti teroristického obsahu v rámci svých služeb.

(23) Při zavádění zvláštních opatření by měli poskytovatelé hostingových služeb zajistit, aby bylo zachováno právo uživatelů na svobodu projevu a informací, jakož i svoboda a pluralita sdělovacích prostředků, jak jsou chráněny Listinou. Kromě požadavků stanovených právními předpisy, včetně právních předpisů na ochranu osobních údajů, by měli poskytovatelé hostingových služeb jednat s náležitou péčí a v příslušných případech zavést záruky, ve vhodných případech včetně lidského dohledu a ověřování, s cílem vyhnout se neúmyslným a chybným rozhodnutím vedoucím k odstranění obsahu, který není teroristickým obsahem, nebo ke znemožnění přístupu k němu.

([10]) 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, s. 73).

(24) Poskytovatel hostingových služeb by měl příslušnému orgánu oznamovat zavedená zvláštní opatření, aby mohl tento orgán určit, zda jsou opatření účinná a přiměřená a zda, jsou-li využívány automatizované prostředky, má poskytovatel hostingových služeb k dispozici nezbytné kapacity lidského dohledu a ověřování. Při posuzování účinnosti a přiměřenosti opatření by příslušné orgány měly zohlednit relevantní parametry včetně počtu příkazů k odstranění obsahu vydaných vůči poskytovateli hostingových služeb, velikosti a ekonomických možností poskytovatele hostingových služeb a dopadů jeho služeb z hlediska šíření teroristického obsahu, například podle počtu uživatelů v Unii, jakož i záruky zavedené proti zneužívání jeho služeb k šíření teroristického obsahu online.

(25) Považuje-li příslušný orgán zavedená zvláštní opatření za nedostatečná k řešení rizik, měl by mít možnost požadovat přijetí dodatečných vhodných, účinných a přiměřených zvláštních opatření. Požadavek na provedení takových dodatečných zvláštních opatření by neměl vést k obecné povinnosti dohledu nebo povinnosti aktivně vyhledávat skutečnosti ve smyslu čl. 15 odst. 1 směrnice 2000/31/ES, ani k povinnosti používat automatizované nástroje. Nicméně poskytovatelé hostingových služeb by měli mít možnost používat automatizované nástroje, pokud to považují za vhodné a nezbytné k účinnému řešení zneužívání svých služeb k šíření teroristického obsahu.

(26) Povinnost poskytovatelů hostingových služeb zachovávat odstraněný obsah a související údaje by měla být uložena pro konkrétní účely a časově omezena na nezbytnou dobu. Požadavek na zachovávání je třeba rozšířit na související údaje v rozsahu, ve kterém by jinak v důsledku odstranění dotyčného teroristického obsahu došlo ke ztrátě takových údajů. Související údaje mohou mimo jiné obsahovat údaje o účastníkovi, zejména údaje týkající se totožnosti poskytovatele obsahu, či údaje o přístupu, například údaje o datu a času použití poskytovatelem obsahu a přihlášení ke službě či odhlášení z ní, společně s IP adresou přidělenou poskytovateli obsahu poskytovatelem služby přístupu na internet.

(27) Povinnost zachovávat obsah pro účely správního či soudního přezkumného řízení je nutná a důvodná, mají-li být zajištěny účinné prostředky nápravy pro poskytovatele obsahu, jejichž obsah byl odstraněn nebo k němu byl znemožněn přístup, a má-li být zajištěno obnovení daného obsahu v závislosti na výsledku uvedených řízení. Povinnost zachovávat materiál pro účely vyšetřování nebo stíhání je důvodná a nutná s ohledem na hodnotu, kterou by mohl tento materiál mít pro účely narušení či prevence teroristické činnosti. Proto by zachovávání odstraněného teroristického obsahu pro účely prevence, odhalování, vyšetřování a stíhání teroristických trestných činů mělo být rovněž považováno za důvodné. Teroristický obsah a s ním spojené údaje měly být zachovávány pouze po nezbytnou dobu umožňující donucovacím orgánům teroristický obsah zkontrolovat a rozhodnout, zda ho bude pro uvedené účely zapotřebí. Pro účely prevence, odhalování, vyšetřování a stíhání teroristických trestných činů by vyžadované zachovávání mělo být omezeno na údaje, které jsou pravděpodobně spojeny s teroristickými trestnými činy, a mohly by tudíž přispět ke stíhání teroristických trestných činů nebo prevenci závažných rizik pro veřejnou bezpečnost. Pokud poskytovatelé hostingových služeb odstraní materiál nebo znemožní přístup k němu zejména prostřednictvím svých zvláštních opatření, měli by neprodleně informovat příslušné orgány o obsahu, který zahrnuje informace ohledně bezprostředního ohrožení života nebo podezření na teroristický trestný čin.

(28) V zajištění přiměřenosti by lhůta pro zachovávání měla být omezena na šest měsíců, aby měli poskytovatelé obsahu dostatečný čas na zahájení příslušného správního či soudního přezkumného řízení nebo aby byl donucovacím orgánům umožněn přístup k relevantním údajům pro účely vyšetřování a stíhání teroristických trestných činů. Tuto lhůtu by ovšem mělo být možné na žádost příslušného orgánu nebo soudu prodloužit na nezbytnou dobu, pokud jsou zmíněná řízení zahájena, ale nejsou v uvedené šestiměsíční lhůtě ukončena. Doba zachovávání by měla být dostatečná, aby umožnila donucovacím orgánům zachovat nezbytný materiál související s vyšetřováním a stíháním a současně zajistila rovnováhu ve vztahu k základním právům.

(29) Tímto nařízením by neměly být dotčeny procesní záruky ani procesní vyšetřovací opatření vztahující se k přístupu k obsahu a souvisejícím údajům zachovávaným pro účely vyšetřování a stíhání teroristických trestných činů, jak jsou upraveny právem Unie nebo vnitrostátním právem.

(30) Pro posílení odpovědnosti poskytovatelů hostingových služeb vůči uživatelům a pro posílení důvěry občanů v jednotný digitální trh je zásadní, aby politiky těchto poskytovatelů týkající se teroristického obsahu byly transparentní. Poskytovatelé hostingových služeb, kteří v daném kalendářním roce přijali, nebo se od nich požadovalo, aby přijali kroky podle tohoto nařízení, by měli zveřejňovat výroční zprávy o transparentnosti obsahující informace o krocích přijatých v souvislosti s identifikací a odstraňováním teroristického obsahu.

(31) Příslušné orgány by měly zveřejňovat výroční zprávy o transparentnosti obsahující informace o počtu příkazů k odstranění, počtu případů, kdy příkaz nebyl proveden, počtu rozhodnutí o zvláštních opatřeních, počtu případů podléhajících správnímu nebo soudnímu přezkumnému řízení a počtu rozhodnutí o uložení sankcí.

(32) Právo na účinnou právní ochranu je zakotveno v článku 19 Smlouvy o Evropské unii (dále jen „Smlouva o EU“) a v článku 47 Listiny. Každá fyzická nebo právnická osoba má právo na účinnou právní ochranu u příslušného vnitrostátního soudu, pokud jde o opatření přijatá na základě tohoto nařízení, která se mohou nepříznivě dotknout práv této osoby. Uvedené právo by mělo zahrnovat zejména možnost pro poskytovatele hostingových služeb a poskytovatele obsahu účinně napadnout příkazy k odstranění nebo rozhodnutí vyplývajícím z přezkumu příkazů k odstranění podle tohoto nařízení u soudu členského státu, jehož příslušné orgány vydaly příkaz k odstranění nebo přijaly rozhodnutí, jakož i možnost pro poskytovatele hostingových služeb účinně napadnout rozhodnutí týkající se zvláštních opatření či sankcí u soudu členského státu, jehož příslušný orgán takové rozhodnutí přijal.

(33) Postupy řešení stížností představují nezbytné záruky proti chybnému odstranění obsahu online nebo znemožnění přístupu k němu, pokud je tento obsah chráněn na základě svobody projevu a informací. Poskytovatelé hostingových služeb by proto měli zavést uživatelsky vstřícné mechanismy pro podávání stížností a zajistit, aby byly stížnosti řešeny urychleně a zcela transparentně ve vztahu k poskytovateli obsahu. Požadavkem, aby poskytovatelé hostingových služeb obnovili obsah, který byl chybně odstraněn nebo k němuž byl chybně znemožněn přístup, by neměla být dotčena možnost, aby poskytovatelé hostingových služeb prosazovali vlastní podmínky.

(34) Účinná právní ochrana v souladu s článkem 19 Smlouvy o EU a článkem 47 Listiny vyžaduje, aby byli poskytovatelé obsahu schopni zjistit důvody, na základě kterých byl jimi poskytnutý obsah odstraněn nebo k němu byl znemožněn přístup. Pro tento účel by měl poskytovatel hostingových služeb poskytovateli obsahu zpřístupnit informace umožňující jeho odstranění nebo znemožnění přístupu k němu napadnout. V závislosti na okolnostech by poskytovatelé hostingových služeb mohli nahradit obsah, který byl odstraněn nebo ke kterému byl znemožněn přístup, sdělením o tom, že obsah byl odstraněn nebo k němu byl znemožněn přístup v souladu s tímto nařízením. Další informace o důvodech odstranění nebo znemožnění přístupu a prostředcích nápravy v případě takového odstranění nebo znemožnění přístupu by měly být poskytnuty na žádost poskytovatele obsahu. Rozhodnou-li se příslušné orgány, že z důvodu veřejné bezpečnosti, a to i v kontextu vyšetřování, je nevhodné či kontraproduktivní informovat o odstranění obsahu nebo znemožnění přístupu k němu přímo poskytovatele obsahu, měli by odpovídajícím způsobem informovat poskytovatele hostingových služeb.

(35) Pro účely tohoto nařízení by měly členské státy určit příslušné orgány. To by nemělo nutně znamenat zřízení nového orgánu a funkcemi stanovenými tímto nařízením by mělo být možné pověřit i některý stávající orgán. Toto nařízení by mělo vyžadovat, aby byly určeny orgány příslušné pro vydávání příkazů k odstranění, přezkum příkazů k odstranění, dohled nad zvláštními opatřeními a ukládání sankcí, přičemž by každý členský stát měl mít možnost rozhodnout o počtu jím určených příslušných orgánů a o tom, zda se bude jednat o orgány správní, donucovací či soudní. Členské státy by měly zajistit, aby příslušné orgány plnily své úkoly objektivně a nediskriminačně a aby v souvislosti s plněním úkolů podle tohoto nařízení nevyžadovaly ani nepřijímaly pokyny od žádného jiného subjektu. To by nemělo bránit dohledu v souladu s vnitrostátním ústavním právem. Členské státy by měly Komisi oznámit příslušné orgány určené podle tohoto nařízení Komisi a ta by měla zveřejnit online rejstřík příslušných orgánů. Tento online rejstřík by měl být snadno dostupný, aby poskytovatelům hostingových služeb usnadnil rychlé ověření pravosti příkazů k odstranění.

(36) Aby se zabránilo zdvojování úsilí a možným zásahům do vyšetřování a minimalizovala se zátěž dotčených poskytovatelů hostingových služeb, měly by si příslušné orgány před vydáním příkazů k odstranění vyměňovat informace, koordinovat činnosti a spolupracovat mezi sebou a případně také s Europolem. Při rozhodování o vydání příkazu k odstranění by měl příslušný orgán náležitě zohlednit jakékoli upozornění na zásah do zájmů vyšetřování („sladění činností"). Je-li příslušný orgán informován příslušným orgánem jiného členského státu o existujícím příkazu k odstranění, neměl by být vydán příkaz k odstranění týkající se téže věci. Při provádění ustanovení tohoto nařízení by Europol mohl poskytovat podporu v souladu se svým mandátem a stávajícím právním rámcem.

(37) Za účelem zajištění účinného a dostatečně soudržného provádění zvláštních opatření přijatých poskytovateli hostingových služeb by příslušné orgány měly koordinovat činnosti a vzájemně spolupracovat, pokud jde o komunikaci s poskytovateli hostingových služeb ohledně příkazů k odstranění a identifikace, provádění a hodnocení zvláštních opatření. Koordinace a spolupráce jsou nutné také ve vztahu k ostatním opatřením pro provádění tohoto nařízení, včetně přijímání a ukládání sankcí. Komise by měla tuto koordinaci a spolupráci usnadňovat.

(38) Je nezbytné, aby byl příslušný orgán členského států zodpovědný za ukládání sankcí v plném rozsahu informován o vydávání příkazů k odstranění a následné komunikaci mezi poskytovatelem hostingových služeb a příslušnými orgány jiných členských států. Pro tento účel by měly členské státy zajistit vhodné a bezpečné komunikační cesty a mechanismy, které umožní včasné sdílení relevantních informací.

(39) Za účelem zprostředkování rychlé komunikace mezi příslušnými orgány a s poskytovateli hostingových služeb a zabránění zdvojování úsilí by členské státy měly být vybízeny k tomu, aby využívaly specializované nástroje vyvinuté Europolem, jako stávající aplikaci pro správu hlášení obsahu na internetu (Internet Referral Management application) nebo nástroje, které ji nahradí.

(40) Jakožto účinný a rychlý způsob, jak zvyšovat informovanost poskytovatelů hostingových služeb o konkrétním obsahu dostupném v rámci jejich služeb a umožnit jim urychleně jednat, se osvědčila hlášení ze strany členských států a Europolu. Tato hlášení, která tvoří mechanismus upozorňování poskytovatelů hostingových služeb na informace, jež by mohly být považovány za teroristický obsah, umožňující poskytovateli hostingových služeb, aby sám dobrovolně posoudil soulad tohoto obsahu s jeho vlastními podmínkami, by měla zůstat k dispozici jako doplněk příkazů k odstranění. Konečné rozhodnutí, zda obsah odstranit, protože není v souladu s podmínkami poskytovatele hostingových služeb, je i nadále na poskytovateli hostingových služeb. Tímto nařízením by neměl být dotčen mandát Europolu stanovený nařízením Evropského parlamentu a Rady (EU) 2016/794 ([11]). Žádné ustanovení tohoto nařízení by proto nemělo být chápáno tak, že členským státům a Europolu brání používat hlášení jako nástroj pro potírání teroristického obsahu online.

(41) S ohledem na obzvláště závažné důsledky některého teroristického obsahu online by poskytovatelé hostingových služeb měli neprodleně informovat relevantní orgány v dotčeném členském státě nebo příslušné orgány členského státu, kde jsou usazeni nebo mají právního zástupce, o teroristickém obsahu, který obnáší bezprostřední ohrožení života nebo podezření na teroristický trestný čin. Za účelem zajištění proporcionality by se tato povinnost měla omezovat na teroristické trestné činy vymezené v čl. 3 odst. 1 směrnice (EU) 2017/541. Z této povinnosti informovat by neměla vyplývat povinnost poskytovatelů hostingových služeb aktivně vyhledávat důkazy takového bezprostředního ohrožení života nebo podezření na teroristický trestný čin. Za dotčený členský stát by měl být považován členský stát, který je příslušný pro vyšetřování a stíhání uvedených teroristických trestných činů na základě státní příslušnosti pachatele nebo potenciální oběti trestného činu nebo cílového místa teroristického činu. V případě pochybností by měli poskytovatelé hostingových služeb předat informace Europolu, který by měl podniknout příslušné kroky v souladu se svým mandátem, což obnáší i předání informace relevantním vnitrostátním orgánům. Příslušné orgány členských států by měly mít možnost využívat takové informace k přijetí vyšetřovacích opatření dostupných podle práva Unie nebo vnitrostátního práva.

([11]) Nařízení Evropského parlamentu a Rady (EU) 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, s. 53).

(42) Poskytovatelé hostingových služeb by měli určit nebo zřídit kontaktní místa, která umožní rychlé zpracování příkazů k odstranění obsahu. Kontaktní místo by mělo sloužit pouze k provozním účelům. Kontaktní místo by mělo sestávat z vyhrazeného prostředku, interního nebo externího, který umožní elektronické podávání příkazů k odstranění, a z technických nebo personálních prostředků umožňujících jejich rychlé zpracování. Není nutné, aby se kontaktní místo nacházelo v Unii. Poskytovatel hostingových služeb by měl mít možnost využít stávající kontaktní místo i pro účely tohoto nařízení, pokud je takové kontaktní místo schopno plnit funkce stanovené tímto nařízením. K zajištění toho, aby byl teroristický obsah odstraněn nebo byl k němu znemožněn přístup do jedné hodiny od přijetí příkazu k odstranění, mělo by být kontaktní místo poskytovatelů hostingových služeb vystavených teroristickému obsahu nepřetržitě dostupné. 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 jsou poskytovatelé hostingových služeb vybízeni k tomu, aby umožnili komunikaci v jednom z úředních jazyků orgánů Unie, ve kterém jsou dostupné jejich podmínky.

(43) Protože neexistuje obecný požadavek, aby poskytovatelé hostingových služeb zajistili fyzickou přítomnost na území Unie, je nutné jednoznačně určit členský stát, do jehož jurisdikce poskytovatel hostingových služeb nabízející služby v Unii spadá. Obecně platí, že poskytovatel hostingových služeb spadá do příslušnosti členského státu, v němž má hlavní provozovnu nebo v němž má jeho právní zástupce bydliště či je usazen. Tím by neměla být dotčena pravidla týkající se příslušnosti pro účely příkazů k odstranění a rozhodnutí vyplývajících z přezkumu příkazů k odstranění podle tohoto nařízení. Pokud však jde o poskytovatele hostingových služeb, který nemá v Unii žádnou provozovnu ani neurčil právního zástupce, měl by mít jurisdikci, a tedy možnost ukládat sankce kterýkoliv členský stát, a to za předpokladu, že je respektována zásada *ne bis in idem*.

(44) Poskytovatelé hostingových služeb, kteří nemají provozovnu v Unii, by měli písemně určit právního zástupce, aby zajistili plnění povinností stanovených tímto nařízením a jejich vymáhání. Poskytovatelé hostingových služeb by měli mít možnost určit pro účely tohoto nařízení právního zástupce, který je již určen i pro jiné účely, a to za předpokladu, že tento právní zástupce je schopen plnit funkce stanovené v tomto nařízení. Právní zástupce by měl být zmocněn jednat jménem poskytovatele hostingových služeb.

(45) Sankce jsou nezbytné k zajištění účinného provádění tohoto nařízení poskytovateli hostingových služeb. Členské státy by měly přijmout pravidla pro sankce, jež mohou být správní či trestní povahy, a v příslušných případech i vodítka pro ukládání pokut. Neplnění povinností v jednotlivých případech by mohlo podléhat sankcím při zohlednění zásady *ne bis in idem* a zásady proporcionality a při zajištění toho, že takové sankce zohledňují soustavná selhání. Sankce by mohly mít různou formu, včetně formálních upozornění v případě méně závažných porušení nebo finančních postihů v souvislosti se závažnějšími nebo soustavnými porušeními. Obzvláště přísné sankce by měly být ukládány v případě, že poskytovatel hostingových služeb soustavně neplní povinnost odstraňovat teroristický obsah či znemožňovat přístup k němu do jedné hodiny od přijetí příkazu k odstranění. Za účelem zajištění právní jistoty by mělo toto nařízení stanovit, která porušení podléhají sankcím a jaké okolnosti jsou významné pro posouzení druhu a výše takové sankce. Při stanovování, zda uložit finanční postih, je třeba náležitým způsobem zohlednit finanční situaci poskytovatele hostingových služeb. Příslušný orgán by navíc měl vzít v úvahu, zda je poskytovatel hostingových služeb začínajícím podnikem (start-up) nebo mikropodnikem či malým a středním podnikem ve smyslu doporučení Komise 2003/361/ES ([12]). Měly by se rovněž zohlednit další okolnosti, jako například to, zda bylo jednání poskytovatele hostingových služeb objektivně neuvážené nebo zavrženíhodné či zda k porušení došlo z nedbalosti, nebo úmyslně. Členské státy by měly zajistit, aby sankce uložené za porušení tohoto nařízení nemotivovaly k odstraňování materiálu, který není teroristickým obsahem.

(46) Spolupráci a výměnu informací mezi příslušnými orgány a poskytovateli hostingových služeb usnadňuje používání standardizovaných vzorů a umožňuje jim rychlejší a účelnější komunikaci. Obzvláště důležité je zajistit po přijetí příkazů k odstranění rychlé provedení opatření. Vzory snižují náklady na překlad a přispívají k vyššímu standardu daného postupu. Vzory pro odpovědi umožňují standardizovanou výměnu informací a jsou obzvláště důležité v případech, kdy nejsou poskytovatelé hostingových služeb schopni splnit příkaz k odstranění. Ověřené kanály pro předkládání dokumentů mohou zaručit autentičnost příkazů k odstranění obsahu, a to včetně přesnosti data a času odeslání a přijetí příkazu.

([12]) Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

(47) Za účelem provádění nezbytných rychlých změn obsahu vzorů, které mají být používány pro účely tohoto nařízení, by měla být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování Evropské unie, pokud jde o změny příloh tohoto nařízení. Za účelem možnosti zohlednění technologického rozvoje a vývoje souvisejícího právního rámce by na Komisi měla být rovněž přenesena pravomoc přijímat akty v přenesené pravomoci, s cílem doplnit toto nařízení o technické požadavky na elektronické prostředky využívané příslušnými orgány k předávání příkazů k odstranění. 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 ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů ([13]). 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 zasedání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

(48) Členské státy by měly shromažďovat informace o provádění tohoto nařízení. Členské státy by měly mít možnost využívat zprávy o transparentnosti poskytovatelů hostingových služeb a v případě potřeby je doplnit o podrobnější informace, jako jsou jejich vlastní zprávy o transparentnosti podle tohoto nařízení. Za účelem získání informací pro hodnocení provádění tohoto nařízení by měl být stanoven podrobný program monitorování výstupů, výsledků a dopadů tohoto nařízení.

(49) Na základě zjištění a závěrů zprávy o provádění a výsledku monitorování by měla Komise provést hodnocení tohoto nařízení, a to do tří let od jeho vstupu v platnost. Hodnocení by mělo být založeno na kritériích účelnosti, nezbytnosti, účinnosti, proporcionality, relevantnosti, soudržnosti a přidané hodnoty Unie. Mělo by posoudit fungování různých provozních a technických opatření stanovených tímto nařízením, a to včetně účinnosti opatření pro zlepšení odhalování, identifikace a odstraňování teroristického obsahu online, účinnosti záruk a dopadů na potenciálně dotčená základní práva, jako jsou svoboda projevu a informací, včetně svobody a plurality sdělovacích prostředků, svobody podnikání a práva na soukromí a ochranu osobních údajů. Komise by měla rovněž posoudit dopad na potenciálně dotčené zájmy třetích stran.

(50) Jelikož cíle tohoto nařízení, totiž zajištění hladkého fungování jednotného digitálního trhu zaměřením se na potírání šíření teroristického obsahu online, nemůže být dosaženo uspokojivě členskými státy, ale spíše jich, z důvodu jeho rozsahu a účinků, může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o EU. 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 týkající se boje proti zneužívání hostingových služeb k veřejnému šíření teroristického obsahu online, zejména pokud jde o:

a) opodstatněné a přiměřené povinnosti náležité péče, které mají poskytovatelé hostingových služeb uplatňovat s cílem potírat veřejné šíření teroristického obsahu prostřednictvím jejich služeb a v případě potřeby zajistit rychlé odstranění tohoto obsahu nebo znemožnění přístupu k němu;

([13]) Úř. věst. L 123, 12.5.2016, s. 1.

b) opatření, která mají členské státy zavést v souladu s právem Unie a s výhradou vhodných záruk na ochranu základních práv, zejména svobodu projevu a informací v otevřené a demokratické společnosti, s cílem:

i) identifikovat teroristický obsah a zajistit jeho rychlé odstranění poskytovateli hostingových služeb a

ii) usnadnit spolupráci mezi příslušnými orgány členských států, poskytovateli hostingových služeb a případně Europolem.

2. Toto nařízení se vztahuje na poskytovatele hostingových služeb nabízející služby v Unii, pokud veřejně šíří informace, bez ohledu na místo, kde mají svou hlavní provozovnu.

3. Veřejně šířený materiál pro vzdělávací, žurnalistické, umělecké nebo výzkumné účely nebo pro účely předcházení terorismu nebo boje proti němu, včetně materiálu, který je vyjádřením polemických či kontroverzních názorů ve veřejné diskusi, se za teroristický obsah nepovažuje. Skutečný účel šíření a to, zda je veřejně šířen materiál k uvedeným účelům, se určí posouzením.

4. Tímto nařízením není dotčena povinnost ctít práva, svobody a zásady uvedené v článku 6 Smlouvy o EU a uplatňuje se, aniž jsou dotčeny základní zásady týkající se svobody projevu a informací, včetně svobody a plurality sdělovacích prostředků.

5. Tímto nařízením nejsou dotčeny směrnice 2000/31/ES a 2010/13/EU. Ve vztahu k audiovizuálním mediálním službám ve smyslu čl. 1 odst. 1 písm. a) směrnice 2010/13/EU má přednost směrnice 2010/13/EU.

Článek 2

Definice

Pro účely tohoto nařízení se rozumí:

1) „poskytovatelem hostingových služeb“ poskytovatel služeb vymezených v čl. 1 písm. b) směrnice Evropského parlamentu a Rady (EU) 2015/1535 ([14]) a spočívajících v uchovávání informací poskytovaných poskytovatelem obsahu a na jeho žádost;

2) „poskytovatelem obsahu“ uživatel, který poskytl informace, které jsou nebo byly poskytovatelem hostingových služeb uloženy a veřejně šířeny;

3) „veřejným šířením“ zpřístupňování informací na žádost poskytovatele obsahu potenciálně neomezenému počtu osob;

4) „nabízením služeb v Unii“ umožnění fyzickým nebo právnickým osobám v jednom nebo více členských státech využívat služeb poskytovatele hostingových služeb, který má významné spojení s tímto členským státem nebo těmito členskými státy;

5) „významným spojením“ spojení poskytovatele hostingových služeb s jedním nebo více členskými státy vyplývající buď z jeho usazení v Unii, nebo z konkrétních kritérií, jakými jsou:

a) významný počet uživatelů jeho služeb v jednom nebo více členských státech; nebo

b) zaměření jeho činností na jeden nebo více členských států;

6) „teroristickými trestnými činy“ trestné činy vymezené v článku 3 směrnice (EU) 2017/541;

([14]) Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti norem a technických předpisů a předpisů pro služby informační společnosti (Úř. věst. L 241, 17.9.2015, s. 1).

7) „teroristickým obsahem“ jeden nebo více z těchto druhů materiálu, totiž materiál, který:

a) podněcuje ke spáchání některého z trestných činů uvedených v čl. 3 odst. 1 písm. a) až i) směrnice (EU) 2017/541, pokud takový materiál přímo či nepřímo, například formou glorifikace teroristických činů, obhajuje páchání teroristických trestných činů, a vyvolává tím nebezpečí, že může být jeden či více takových trestných činů spáchán;

b) získává osobu nebo skupinu osob ke spáchání nebo přispění ke spáchání některého z trestných činů uvedených v čl. 3 odst. 1 písm. a) až i) směrnice (EU) 2017/541;

c) získává osobu nebo skupinu osob k účasti na činnostech teroristické skupiny ve smyslu čl. 4 písm. b) směrnice (EU) 2017/541;

d) poskytuje návod k výrobě nebo použití výbušnin, palných nebo jiných zbraní nebo škodlivých či nebezpečných látek, nebo k jiným specifickým metodám či technikám za účelem spáchání nebo přispění ke spáchání některého z trestných činů uvedených v čl. 3 odst. 1 písm. a) až i) směrnice (EU) 2017/541;

e) vyhrožuje spácháním některého z trestných činů uvedených v čl. 3 odst. 1 písm. a) až i) směrnice (EU) 2017/541;

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

9) „hlavní provozovnou“ ústředí nebo sídlo poskytovatele hostingových služeb, v němž jsou vykonávány hlavní finanční funkce a provozní kontrola.

ODDÍL II

OPATŘENÍ ZAMĚŘENÁ NA POTÍRÁNÍ ŠÍŘENÍ TERORISTICKÉHO OBSAHU ONLINE

Článek 3

Příkazy k odstranění

1. Příslušný orgán každého členského státu je oprávněn vydat příkaz k odstranění, kterým se od poskytovatelů hostingových služeb požaduje, aby odstranili teroristický obsah nebo znemožnili přístup k teroristickému obsahu ve všech členských státech.

2. Pokud příslušný orgán již dříve nevydal poskytovateli hostingové služby příkaz k odstranění, poskytne tomuto poskytovateli hostingových služeb alespoň dvanáct hodin před vydáním příkazu k odstranění informace o platných postupech a lhůtách.

První pododstavec se nepoužije v řádně odůvodněných naléhavých případech.

3. Poskytovatelé hostingových služeb odstraní teroristický obsah nebo znemožní přístup k teroristickému obsahu ve všech členských státech co nejdříve a v každém případě do jedné hodiny od přijetí příkazu k odstranění.

4. Příslušné orgány použijí k vydávání příkazů k odstranění vzor uvedený v příloze I. Příkazy k odstranění obsahují tyto prvky:

a) identifikační údaje příslušného orgánu, který vydává příkaz k odstranění, a autentizaci příkazu k odstranění ze strany tohoto příslušného orgánu;

b) dostatečně podrobné odůvodnění, proč je obsah považován za teroristický obsah, a odkaz na příslušný druh materiálu podle čl. 2 bodu 7;

c) přesný jednotný lokátor zdroje (URL) a v případě potřeby další informace k identifikaci teroristického obsahu;

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

e) datum, razítko s časem vydání a elektronický podpis příslušného orgánu vydávajícího příkaz k odstranění;

f) snadno srozumitelné informace o prostředcích nápravy, které jsou poskytovateli hostingových služeb a poskytovateli obsahu k dispozici, včetně informací o prostředcích nápravy u příslušného orgánu, možnosti obrátit se na soud a lhůt pro odvolání;

g) je-li to nezbytné a přiměřené, rozhodnutí nezveřejnit informace o odstranění teroristického obsahu nebo o znemožnění přístupu k němu v souladu s čl. 11 odst. 3.

5. Příslušný orgán zašle příkazy k odstranění do hlavní provozovny poskytovatele hostingových služeb nebo jeho právnímu zástupci určenému v souladu s článkem 17.

Příslušný orgán předá příkaz k odstranění kontaktnímu místu uvedenému v čl. 15 odst. 1, a to elektronickými prostředky, které dovolují vytvořit písemný záznam za podmínek umožňujících autentizaci odesílatele, včetně přesnosti data a času odeslání a přijetí příkazu.

6. Poskytovatel hostingových služeb bez zbytečného odkladu informuje příslušný orgán o odstranění teroristického obsahu nebo o znemožnění přístupu k teroristickému obsahu ve všech členských státech a uvede zejména čas, kdy bylo odstranění nebo znemožnění přístupu provedeno, přičemž použije vzor uvedený v příloze II.

7. Pokud poskytovatel hostingových služeb nemůže příkaz k odstranění splnit z důvodu vyšší moci nebo faktické nemožnosti, za kterou poskytovatel hostingových služeb neodpovídá, včetně objektivně opodstatněných technických nebo provozních důvodů, informuje bez zbytečného odkladu o tomto důvodu příslušný orgán, který vydal příkaz k odstranění, přičemž použije vzor uvedený v příloze III.

Lhůta stanovená v odstavci 3 začíná běžet, jakmile pomine důvod uvedený v prvním pododstavci tohoto odstavce.

8. Pokud poskytovatel hostingových služeb nemůže příkaz k odstranění splnit, protože obsahuje zjevné chyby nebo neobsahuje dostatečné informace pro jeho provedení, informuje o tom bez zbytečného odkladu příslušný orgán, který příkaz k odstranění vydal, a požádá o nezbytné vysvětlení, přičemž použije vzor uvedený v příloze III.

Lhůta uvedená v odstavci 3 začíná běžet, jakmile poskytoval hostingových služeb obdrží nezbytné vysvětlení.

9. Příkaz k odstranění se stane pravomocným po uplynutí lhůty pro odvolání, pokud nebylo podáno žádné odvolání v souladu s vnitrostátním právem, nebo po jeho potvrzení v případě odvolání.

Jakmile se příkaz k odstranění stane pravomocným, příslušný orgán, který tento příkaz k odstranění vydal, o tom informuje příslušný orgán uvedený v čl. 12 odst. 1 písm. c) členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má bydliště nebo je usazen jeho právní zástupce.

Článek 4

Postup u přeshraničních příkazů k odstranění

1. S výhradou článku 3, pokud poskytovatel hostingových služeb nemá hlavní provozovnu nebo právního zástupce v členském státě příslušného orgánu, který vydal příkaz k odstranění, předá tento orgán současně kopii příkazu k odstranění příslušnému orgánu členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má bydliště nebo je usazen jeho právní zástupce.

2. Pokud poskytovatel hostingových služeb obdrží příkaz k odstranění podle tohoto článku, přijme opatření uvedená v článku 3 a učiní nezbytné kroky k tomu, aby byl schopen obsah obnovit nebo k němu znovu umožnit přístup v souladu s odstavcem 7 tohoto článku.

3. Příslušný orgán členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má bydliště nebo je usazen jeho právní zástupce, může z vlastního podnětu do 72 hodin od obdržení kopie příkazu k odstranění podle odstavce 1 tento příkaz k odstranění přezkoumat s cílem určit, zda závažně nebo zjevně neporušuje toto nařízení nebo základní práva a svobody zaručené Listinou.

Pokud takové porušení zjistí, přijme v téže lhůtě odpovídající odůvodněné rozhodnutí.

4. Poskytovatelé hostingových služeb a poskytovatelé obsahu jsou oprávněni do 48 hodin od obdržení příkazu k odstranění, nebo informace podle čl. 11 odst. 2, podat příslušnému orgánu členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má bydliště nebo je usazen jeho právní zástupce, odůvodněnou žádost o přezkum příkazu k odstranění podle odstavce 3 prvního pododstavce tohoto článku.

Po provedení přezkumu příkazu k odstranění přijme příslušný orgán do 72 hodin od obdržení žádosti odůvodněné rozhodnutí, v němž uvede, zda podle jeho zjištění k porušení došlo.

5. Příslušný orgán před přijetím rozhodnutí podle odst. 3 druhého pododstavce nebo rozhodnutí o porušení podle odst. 4 druhého pododstavce informuje příslušný orgán, který vydal příkaz k odstranění, o svém záměru přijmout rozhodnutí a o důvodech, které jej k tomu vedou.

6. Pokud příslušný orgán členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má bydliště nebo je usazen jeho právní zástupce, přijme odůvodněné rozhodnutí v souladu s odstavcem 3 nebo 4 tohoto článku, neprodleně toto rozhodnutí sdělí příslušnému orgánu, který vydal příkaz k odstranění, poskytovateli hostingových služeb, poskytovateli obsahu, který požádal o přezkum podle odstavce 4 tohoto článku, a v souladu s článkem 14 Europolu. Pokud rozhodnutí podle odstavce 3 nebo 4 tohoto článku konstatuje porušení, pozbývá příkaz k odstranění právních účinků.

7. Poté, co dotčený poskytovatel hostingových služeb obdrží v souladu s odstavcem 6 rozhodnutí konstatující porušení, okamžitě obnoví obsah nebo k němu znovu umožní přístup, aniž je dotčena možnost, aby vymáhal své podmínky v souladu s unijním a vnitrostátním právem.

Článek 5

Zvláštní opatření

1. Poskytovatel hostingových služeb vystavený teroristickému obsahu podle odstavce 4 v příslušných případech zahrne do svých podmínek ustanovení týkající se zneužívání jeho služeb k veřejnému šíření teroristického obsahu a tato ustanovení uplatňuje.

Učiní tak řádným, přiměřeným a nediskriminačním způsobem a za všech okolností s patřičným ohledem na základní práva uživatelů a vezme přitom v úvahu zejména zásadní význam svobody projevu a informací v otevřené a demokratické společnosti, s cílem vyhnout se odstranění jiného než teroristického obsahu.

2. Poskytovatel hostingových služeb vystavený teroristickému obsahu podle odstavce 4 přijme zvláštní opatření na ochranu svých služeb proti veřejnému šíření teroristického obsahu.

O zvláštních opatřeních rozhoduje poskytovatel hostingových služeb. Takováto opatření mohou zahrnovat jedno nebo více z těchto opatření:

a) vhodná technická a provozní opatření nebo kapacity, jako například odpovídající personál nebo technické prostředky pro identifikaci a rychlé odstraňování teroristického obsahu nebo znemožnění přístupu k němu;

b) snadno dostupné a uživatelsky vstřícné mechanismy, jejichž prostřednictvím mohou uživatelé poskytovateli hostingových služeb oznamovat nebo označovat domnělý teroristický obsah;

c) jakékoli jiné mechanismy ke zvýšení informovanosti o teroristickém obsahu v rámci jeho služeb, jako jsou mechanismy uživatelského moderování;

d) jakékoli jiné opatření, které poskytovatel hostingových služeb považuje za vhodné pro potírání dostupnosti teroristického obsahu v rámci svých služeb.

3. Zvláštní opatření musí splňovat všechny tyto požadavky:

a) jsou účinná při zmírňování míry vystavení služeb poskytovatele hostingových služeb teroristickému obsahu;

b) jsou cílená a přiměřená, zejména se zohledněním závažnosti míry vystavení služeb poskytovatele hostingových služeb teroristickému obsahu, jakož i technických a provozních kapacit, finanční síly, počtu uživatelů služeb poskytovatele hostingových služeb a objemu jimi poskytovaného obsahu;

c) jsou uplatňována způsobem, při němž se plně zohledňují práva a oprávněné zájmy uživatelů, zejména základní práva uživatelů na svobodu projevu a informací, na respektování soukromého života a na ochranu osobních údajů;

d) jsou uplatňována s řádnou péčí a nediskriminačně.

Pokud zvláštní opatření zahrnují použití technických opatření, zavedou se vhodné a účinné záruky, které zajistí přesnost a zabrání odstranění materiálu, který není teroristickým obsahem, zejména prostřednictvím lidského dohledu a ověřování.

4. Poskytovatel hostingových služeb je vystaven teroristickému obsahu, pokud příslušný orgán členského státu, v němž má tento poskytovatel hlavní provozovnu nebo v němž má bydliště nebo je usazen jeho právní zástupce,

a) přijal rozhodnutí založené na objektivních faktorech, například na skutečnosti, že poskytovatel hostingových služeb v předchozích dvanácti měsících obdržel dva nebo více pravomocných příkazů k odstranění, kterým konstatuje, že poskytovatel hostingových služeb je vystaven teroristickému obsahu a

b) oznámil rozhodnutí uvedené v písmenu a) poskytovateli hostingových služeb.

5. Po obdržení rozhodnutí uvedeného v odstavci 4 nebo případně v odstavci 6 oznámí poskytovatel hostingových služeb příslušnému orgánu zvláštní opatření, která přijal a která hodlá přijmout k zajištění souladu s odstavci 2 a 3. Učiní tak do tří měsíců od obdržení rozhodnutí a poté každý rok. Tato povinnost zaniká, jakmile příslušný orgán v návaznosti na žádost podle odstavce 7 rozhodne, že poskytovatel hostingových služeb již není vystaven teroristickému obsahu.

6. Pokud se příslušný orgán na základě oznámení uvedených v odstavci 5 a případně jakýchkoli jiných objektivních faktorů domnívá, že přijatá zvláštní opatření nejsou v souladu s odstavci 2 a 3, zašle poskytovateli hostingových služeb rozhodnutí, jímž mu uloží, aby přijal nezbytná opatření k zajištění souladu s odstavci 2 a 3.

Poskytovatel hostingových služeb může sám rozhodnout o druhu zvláštních opatření, která přijme.

7. Poskytovatel hostingových služeb může příslušný orgán kdykoli požádat, aby rozhodnutí podle odstavců 4 nebo 6 přezkoumal a případně změnil nebo zrušil.

Příslušný orgán do tří měsíců od obdržení žádosti přijme ohledně této žádosti odůvodněné rozhodnutí založené na objektivních faktorech a oznámí je poskytovateli hostingových služeb.

8. Žádným požadavkem na přijetí zvláštních opatření není dotčen čl. 15 odst. 1 směrnice 2000/31/ES a nevyplývá z něj ani obecná povinnost poskytovatelů hostingových služeb dohlížet na jimi přenášené nebo ukládané informace, ani obecná povinnost aktivně vyhledávat skutečnosti nebo okolnosti poukazující na protiprávní činnost.

Žádný požadavek na přijetí zvláštních opatření nezahrnuje povinnost poskytovatele hostingových služeb používat automatizované nástroje.

Článek 6

Zachovávání obsahu a souvisejících údajů

1. Poskytovatelé hostingových služeb zachovávají teroristický obsah, který byl odstraněn nebo k němuž byl znemožněn přístup v důsledku příkazu k odstranění podle článku 3 nebo zvláštních opatření podle článku 5, jakož i související údaje, jež byly odstraněny v důsledku odstranění teroristického obsahu, jež jsou nutné pro účely:

a) právního či soudního přezkumného řízení nebo vyřizování stížností podle článku 10 proti rozhodnutím o odstranění teroristického obsahu a souvisejících údajů nebo znemožnění přístupu k nim; nebo

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

2. Teroristický obsah a související údaje uvedené v odstavci 1 se zachovávají po dobu šesti měsíců od jejich odstranění nebo znemožnění přístupu k nim. Teroristický obsah se na žádost příslušného orgánu nebo soudu zachovává po další stanovenou dobu, pouze pokud je to nezbytné pro účely probíhajících správních či soudních přezkumných řízení uvedených v odst. 1 písm. a).

3. Poskytovatelé hostingových služeb zajistí, aby se na teroristický obsah a související údaje zachovávané podle odstavce 1 vztahovaly vhodné technické a organizační záruky.

Tyto technické a organizační záruky zajistí, aby byly zachovávaný 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 tato ochranná opatření v případě potřeby přezkoumají a aktualizují.

ODDÍL III

OCHRANNÁ OPATŘENÍ A ODPOVĚDNOST

Článek 7

Povinnosti poskytovatelů hostingových služeb týkající se transparentnosti

1. Poskytovatelé hostingových služeb ve svých podmínkách jasně vymezí svou politiku zaměřenou na potírání šíření teroristického obsahu, přičemž v příslušných případech mimo jiné věcně vysvětlí fungování zvláštních opatření, včetně případného používání automatizovaných nástrojů.

2. Poskytovatel hostingových služeb, který v daném kalendářním roce přijal opatření proti šíření teroristického obsahu, nebo se od něj požadovalo, aby přijal opatření podle tohoto nařízení, zveřejní za daný rok zprávu o transparentnosti týkající se těchto opatření. Tuto zprávu zveřejní do 1. března následujícího roku.

3. Zprávy o transparentnosti obsahují alespoň tyto údaje:

a) informace o opatřeních poskytovatele hostingových služeb v souvislosti s identifikací a odstraňováním teroristického obsahu nebo znemožňováním přístupu k němu;

b) informace o opatřeních poskytovatele hostingových služeb proti opětovnému online výskytu materiálu, který byl již dříve odstraněn nebo k němuž byl znemožněn přístup, protože byl považován za teroristický obsah, zejména při použití automatizovaných nástrojů;

c) počet položek teroristického obsahu, který byl odstraněn nebo k němuž byl znemožněn přístup na základě příkazů k odstranění či zvláštních opatření, a počet příkazů k odstranění, kdy obsah nebyl odstraněn nebo přístup k němu nebyl znemožněn v souladu s čl. 3 odst. 7 prvním pododstavcem a čl. 3 odst. 8 prvním pododstavcem, společně s odůvodněním;

d) počet a výsledky stížností vyřízených poskytovatelem hostingových služeb v souladu s článkem 10;

e) počet a výsledky správních či soudních přezkumných řízení iniciovaných poskytovatelem hostingových služeb;

f) počet případů, kdy poskytovatel hostingových služeb musel v důsledku správního či soudního přezkumného řízení obnovit obsah nebo k němu znovu umožnit přístup;

g) počet případů, kdy poskytovatel hostingových služeb obnovil obsah nebo k němu znovu umožnil přístup na základě stížnosti poskytovatele obsahu.

Článek 8

Zprávy o transparentnosti příslušných orgánů

1. Příslušné orgány zveřejňují výroční zprávy o transparentnosti týkající se jejich činností podle tohoto nařízení. Tyto zprávy obsahují za daný kalendářní rok přinejmenším tyto informace:

a) počet příkazů k odstranění vydaných podle článku 3, s uvedením počtu příkazů k odstranění podle čl. 4 odst. 1, počet příkazů k odstranění přezkoumaných podle článku 4 a informace o provádění daných příkazů k odstranění dotčenými poskytovateli hostingových služeb, včetně počtu případů, kdy byl teroristický obsah odstraněn nebo přístup k němu znemožněn, a počtu případů, kdy teroristický obsah nebyl odstraněn nebo přístup k němu nebyl znemožněn;

b) počet rozhodnutí přijatých v souladu s čl. 5 odst. 4, 6 nebo 7 a informace o provádění těchto rozhodnutí poskytovateli hostingových služeb, včetně popisu zvláštních opatření;

c) počet případů, kdy byly příkazy k odstranění a rozhodnutí přijatá v souladu s čl. 5 odst. 4 a 6 předmětem správního či soudního přezkumného řízení, a informace o výsledku příslušných řízení;

d) počet rozhodnutí ukládajících sankce podle článku 18 a popis druhu uložené sankce.

2. Výroční zprávy o transparentnosti uvedené v odstavci 1 neobsahují informace, jež by mohly ovlivnit probíhající činnosti v oblasti prevence, odhalování, vyšetřování nebo stíhání teroristických trestných činů nebo zájmy národní bezpečnosti.

Článek 9

Prostředky nápravy

1. Poskytovatelé hostingových služeb, kteří obdrželi příkaz k odstranění vydaný podle čl. 3 odst. 1 nebo rozhodnutí podle čl. 4 odst. 4 nebo podle čl. 5 odst. 4, 6 nebo 7, mají právo na účinnou právní ochranu. Toto právo zahrnuje právo napadnout daný příkaz k odstranění u soudů členského státu příslušného orgánu, který příkaz k odstranění vydal, a právo napadnout rozhodnutí podle čl. 4 odst. 4 nebo podle čl. 5 odst. 4, 6 nebo 7 u soudů členského státu příslušného orgánu, který toto rozhodnutí přijal.

2. Poskytovatelé obsahu, jejichž obsah byl odstraněn nebo k němuž byl znemožněn přístup na základě příkazu k odstranění, mají právo na účinnou právní ochranu. Toto právo zahrnuje právo napadnout příkaz k odstranění vydaný podle čl. 3 odst. 1 u soudů členského státu příslušného orgánu, který příkaz k odstranění vydal, a právo napadnout rozhodnutí podle čl. 4 odst. 4 nebo podle čl. 5 odst. 4, 6 nebo 7 u soudů členského státu příslušného orgánu, který toto rozhodnutí přijal.

3. Členské státy zavedou účinné postupy pro výkon práv uvedených v tomto článku.

Článek 10

Mechanismy pro podávání stížností

1. Každý poskytovatel hostingových služeb zavede účinný a přístupný mechanismus umožňující poskytovatelům obsahu, jejichž obsah byl odstraněn nebo k němuž byl znemožněn přístup v důsledku zvláštních opatření podle článku 5, podat stížnost týkající se odstranění obsahu nebo znemožnění přístupu k němu s žádostí o jeho obnovení nebo znovu-umožnění přístupu k němu.

2. Každý poskytovatel hostingových služeb urychleně prošetří všechny stížnosti, které obdrží prostřednictvím mechanismu uvedeného v odstavci 1, a bez zbytečného odkladu odstraněný obsah obnoví nebo k němu znovu umožní přístup v případech, kdy jeho odstranění či znemožnění přístupu k němu bylo neoprávněné. O výsledku šetření informuje stěžovatele do dvou týdnů od přijetí stížnosti.

Pokud je stížnost zamítnuta, musí o tom poskytovatel hostingových služeb uvědomit stěžovatele a své rozhodnutí odůvodní

Obnovení obsahu nebo znovuumožnění přístupu k němu nevylučuje možnost napadnout rozhodnutí poskytovatele hostingových služeb nebo příslušného orgánu ve správním či soudním přezkumném řízení.

Článek 11

Informace pro poskytovatele obsahu

1. Jestliže poskytovatel hostingových služeb odstraní teroristický obsah nebo k němu znemožní přístup, poskytnout informaci o tomto odstranění či znemožnění přístupu poskytovateli obsahu.

2. Na žádost poskytovatele obsahu jej poskytovatel hostingových služeb buď informuje o důvodech odstranění nebo znemožnění přístupu a o jeho právu napadnout příkaz k odstranění, nebo mu poskytne kopii příkazu k odstranění.

3. Povinnost podle odstavců 1 a 2 se nevztahuje na případy, kdy příslušný orgán vydávající příkaz k odstranění rozhodne, že je nezbytné a přiměřené, aby z důvodu veřejné bezpečnosti, jako je prevence, vyšetřování, odhalování a stíhání teroristických trestných činů, nebyla daná informace zveřejněna, a to po dobu nezbytně nutnou, avšak ne delší než šest týdnů od uvedeného rozhodnutí. V takovém případě poskytovatel hostingových služeb nezveřejní žádné informace o odstranění teroristického obsahu nebo znemožnění přístupu k němu.

Uvedený příslušný orgán může lhůtu prodloužit o dalších šest týdnů, pokud je takové neuveřejňování nadále opodstatněné.

ODDÍL IV

PŘÍSLUŠNÉ ORGÁNY A SPOLUPRÁCE

Článek 12

Určení příslušných orgánů

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

a) vydávání příkazů k odstranění podle článku 3;

b) přezkumu příkazů k odstranění podle článku 4;

c) dohledu nad prováděním zvláštních opatření podle článku 5;

d) ukládání sankcí podle článku 18.

2. Každý členský stát zajistí, aby bylo v rámci příslušného orgánu uvedeného v odst. 1 písm. a) určeno nebo zřízeno kontaktní místo pro vyřizování žádostí o vysvětlení a zpětnou vazbu týkající se příkazů k odstranění vydaných tímto příslušným orgánem.

Členské státy zajistí, aby informace o kontaktním místě byly veřejně dostupné.

3. Členské státy oznámí Komisi příslušný orgán nebo orgány uvedené v odstavci 1 a jejich případné změny do 7. června 2022. Komise oznámení a veškeré jejich změny zveřejní v *Úředním věstníku Evropské unie*.

4. Do 7. června 2022 zřídí Komise online rejstřík příslušných orgánů uvedených v odstavci 1 a kontaktních míst určených nebo zřízených podle odstavce 2 pro každý příslušný orgán. Veškeré změny rejstříku Komise pravidelně zveřejňuje.

Článek 13

Příslušné orgány

1. Členské státy zajistí, aby jejich příslušné orgány měly nezbytné pravomoci a dostatečné zdroje k dosažení cílů tohoto nařízení a plnění svých povinností, které z něj vyplývají.

2. Členské státy zajistí, aby jejich příslušné orgány plnily své úkoly podle tohoto nařízení objektivně a nediskriminačně a při plném dodržování základních práv. Příslušné orgány si v souvislosti s plněním funkcí uvedených v čl. 12 odst. 1 nevyžádají ani nepřijmou pokyny od žádného jiného subjektu.

První pododstavec nebrání dohledu v souladu s vnitrostátním ústavním právem.

Článek 14

Spolupráce mezi poskytovateli hostingových služeb, příslušnými orgány a Europolem

1. Příslušné orgány si ve věci příkazů k odstranění vyměňují informace, koordinují svoji činnost, spolupracují mezi sebou a případně také s Europolem, zejména aby se zabránilo zdvojování úsilí, posílila se koordinace a zabránilo se zásahům do vyšetřování v různých členských státech.

2. Příslušné orgány členských států si ve věci zvláštních opatření přijatých podle článku 5 a sankcí uložených podle článku 18 vyměňují informace s příslušnými orgány uvedenými v čl. 12 odst. 1 písm. c) a d), koordinují s nimi činnost a spolupracují s nimi. Členské státy zajistí, aby příslušné orgány uvedené v čl. 12 odst. 1 písm. c) a d) měly k dispozici veškeré důležité informace.

3. Pro účely odstavce 1 členské státy zajistí vhodné a bezpečné komunikační cesty nebo mechanismy, aby mohly být důležité informace vyměňovány včas.

4. V zájmu účinného provádění tohoto nařízení a zabránění zdvojování úsilí mohou členské státy a poskytovatelé hostingových služeb využívat specializované nástroje, včetně nástrojů zavedených Europolem, a to zejména k usnadnění:

a) zpracování a zpětné vazby, jež se týkají příkazů k odstranění podle článku 3; a

b) spolupráce, jejímž cílem je určit a provádět zvláštní opatření podle článku 5.

5. Pokud se poskytovatelé hostingových služeb dozvědí o teroristickém obsahu, jenž obnáší bezprostřední ohrožení života, neprodleně uvědomí orgány příslušné k vyšetřování a stíhání trestných činů v dotčených členských státech. Není-li možné dotčené členské státy určit, poskytovatelé hostingových služeb uvědomí kontaktní místo podle čl. 12 odst. 2 v členském státě, v němž mají hlavní provozovnu nebo v němž má bydliště nebo je usazen jejich právní zástupce, a předají informace o teroristickém obsahu Europolu za účelem přijetí vhodných následných opatření.

6. Příslušné orgány se vybízejí, aby Europolu zasílaly kopie příkazů k odstranění, které mu umožní předkládat výroční zprávu obsahující analýzy druhů teroristického obsahu, na které se příkazy k odstranění nebo znemožnění přístupu podle tohoto nařízení vztahují.

Článek 15

Kontaktní místa poskytovatelů hostingových služeb

1. Každý poskytovatel hostingových služeb určí nebo zřídí kontaktní místo k přijímání příkazů k odstranění elektronickou cestou a jejich urychlenému zpracování podle článků 3 a 4. Poskytovatel hostingových služeb zajistí, aby informace o kontaktním místě byly veřejně dostupné.

2. V informacích uvedených v odstavci 1 tohoto článku se upřesní úřední jazyky orgánů podle nařízení č. 1/58 ([15]), v nichž je možné se obrátit na kontaktní místo a ve kterých se mají uskutečnit další výměny informací o příkazech k odstranění podle článku 3. Tyto jazyky zahrnují 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.

ODDÍL V

PROVÁDĚNÍ A VYMÁHÁNÍ

Článek 16

Příslušnost

1. Členský stát, v němž má poskytovatel hostingových služeb hlavní provozovnu, je příslušný pro účely článků 5, 18 a 21. Pokud poskytovatel hostingových služeb nemá hlavní provozovnu v Unii, má se za to, že spadá do příslušnosti členského státu, v němž má bydliště nebo je usazen jeho právní zástupce.

2. Pokud poskytovatel hostingových služeb, který nemá hlavní provozovnu v Unii, neurčí svého právního zástupce, jsou příslušné všechny členské státy.

3. Pokud příslušný orgán členského státu vykonává svou příslušnost podle odstavce 2, uvědomí o tom příslušné orgány všech ostatních členských států.

Článek 17

Právní zástupce

1. Poskytovatel hostingových služeb, který nemá hlavní provozovnu v Unii, určí písemně fyzickou, nebo právnickou osobu, která je jeho právním zástupcem v Unii pro účely přijímání, dodržování a vymáhání příkazů k odstranění a rozhodnutí vydaných příslušnými orgány.

2. Poskytovatel hostingových služeb poskytne svému právnímu zástupci nezbytné pravomoci a zdroje pro plnění těchto příkazů k odstranění a rozhodnutí a pro spolupráci s příslušnými orgány.

Právní zástupce má bydliště nebo je usazen v některém z členských států, v nichž poskytovatel hostingových služeb nabízí své služby.

3. Právní zástupce může nést odpovědnost za porušení tohoto nařízení, aniž je tím dotčena odpovědnost poskytovatele hostingových služeb nebo právní kroky vůči němu.

4. Poskytovatel hostingových služeb určení oznámí příslušnému orgánu uvedenému v čl. 12 odst. 1 písm. d) členského státu, v němž má bydliště nebo je usazen jeho právní zástupce.

Poskytovatel hostingových služeb informace o právním zástupci zveřejní.

ODDÍL VI

ZÁVĚREČNÁ USTANOVENÍ

Článek 18

Sankce

1. Členské státy stanoví pravidla pro sankce za porušení tohoto nařízení a přijmou veškerá opatření nezbytná k zajištění jejich uplatňování. Tyto sankce se omezují na porušení čl. 3 odst. 3 a 6, čl. 4 odst. 2 a 7, čl. 5 odst. 1, 2, 3, 5 a 6, článků 6, 7, 10 a 11, čl. 14 odst. 5, čl. 15 odst. 1 a článku 17.

([15]) Nařízení č. 1 o užívání jazyků v Evropském hospodářském společenství (Úř. věst. 17, 6.10.1958, s. 385).

Sankce uvedené v prvním pododstavci musí být účinné, přiměřené a odrazující. Členské státy tato pravidla a opatření oznámí Komisi do 7. června 2022 a neprodleně jí oznámí i všechny jejich následné změny.

2. Členské státy zajistí, aby příslušné orgány při rozhodování o tom, zda uloží sankci, a při určování druhu a výše sankce zohledňovaly všechny významné okolnosti, mimo jiné:

a) povahu, závažnost a dobu trvání porušení;

b) zda došlo k porušení úmyslně, nebo z nedbalosti;

c) předchozí porušení ze strany poskytovatele hostingových služeb;

d) finanční sílu poskytovatele hostingových služeb;

e) míru spolupráce poskytovatele hostingových služeb s příslušnými orgány;

f) povahu a velikost poskytovatele hostingových služeb, zejména v případě mikropodniků a malých a středních podniků;

g) míru pochybení poskytovatele hostingových služeb, se zřetelem k technickým a organizačním opatřením, jež poskytovatel hostingových služeb přijal v zájmu dodržování tohoto nařízení.

3. Členské státy zajistí, aby soustavné či přetrvávající porušování povinností podle čl. 3 odst. 3 podléhalo finančním sankcím ve výši až 4 % celosvětového obratu poskytovatele hostingových služeb v předcházejícím hospodářském roce.

Článek 19

Technické požadavky a změny příloh

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

2. Komisi je svěřena pravomoc přijímat v souladu s článkem 20 akty v přenesené pravomoci za účelem změn příloh, s cílem účinně řešit možnou potřebu zlepšení obsahu vzoru příkazu k odstranění a vzoru pro poskytnutí informace 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 od 7. června 2022.

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v článku 19 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm 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 tehdy, pokud proti němu Evropský parlament ani 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

Monitorování

1. Členské státy shromažďují od svých příslušných orgánů a poskytovatelů hostingových služeb, kteří spadají do jejich jurisdikce, informace o opatřeních, která příslušné orgány a poskytovatelé hostingových služeb přijali v předchozím kalendářním roce v souladu s tímto nařízením, a tyto informace každoročně do 31. března zasílají Komisi. Tyto informace zahrnují:

a) počet vydaných příkazů k odstranění a počet položek teroristického obsahu, který byl odstraněn nebo k němuž byl znemožněn přístup, a rychlost jeho odstranění nebo znemožnění přístupu k němu;

b) zvláštní opatření přijatá podle článku 5, včetně počtu položek teroristického obsahu, který byl odstraněn nebo k němuž byl znemožněn přístup, a rychlosti jeho odstranění nebo znemožnění přístupu k němu;

c) počet žádostí o přístup vydaných příslušnými orgány ve vztahu k obsahu zachovávanému poskytovateli hostingových služeb podle článku 6;

d) počet zahájených postupů pro podávání stížností a opatření přijatá poskytovateli hostingových služeb podle článku 10;

e) počet zahájených správních nebo soudních přezkumných řízení a rozhodnutí přijatá příslušným orgánem v souladu s vnitrostátním právem.

2. Do 7. června 2023 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 dalších důkazů za účelem monitorování výsledků a hodnocení tohoto nařízení podle článku 23.

Článek 22

Zpráva o provádění

Do 7. června 2023 předloží Komise Evropskému parlamentu a Radě zprávu o uplatňování tohoto nařízení. Zpráva obsahuje 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 této zprávy nezbytné.

Článek 23

Hodnocení

Do 7. června 2024 Komise provede hodnocení tohoto nařízení a předloží Evropskému parlamentu a Radě zprávu o jeho uplatňování, včetně:

a) fungování a účinnosti ochranných mechanismů, zejména těch, které jsou uvedeny v čl. 4 odst. 4, čl. 6 odst. 3 a v článcích 7 až 11;

b) dopadů uplatňování tohoto nařízení na základní práva, zejména svobodu projevu a informací, respektování soukromého života a ochranu osobních údajů; a

c) přispění tohoto nařízení k ochraně veřejné bezpečnosti.

Ke zprávě se případně připojí legislativní návrhy.

Členské státy poskytnou Komisi informace, které jsou pro vypracování této zprávy nezbytné.

Komise rovněž posoudí, zda je nezbytné a proveditelné, aby byla v zájmu usnadnění komunikace a spolupráce podle tohoto nařízení zřízena evropská platforma pro teroristický obsah online.

Článek 24

Vstup v platnost a použitelnost

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

Použije se od 7. června 2022.

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

V Bruselu dne 29. dubna 2021.

Za Evropský parlament	*Za Radu*
předseda	*předseda*
D.M. SASSOLI	A.P. ZACARIAS

PŘÍLOHA I

PŘÍKAZ K ODSTRANĚNÍ

(článek 3 nařízení Evropského parlamentu a Rady (EU) 2021/784)

Podle článku 3 nařízení (EU) 2021/784 (dále jen „nařízení“) musí adresát tohoto příkazu k odstranění odstranit teroristický obsah nebo znemožnit přístup k teroristickému obsahu ve všech členských státech, a to co nejdříve a v každém případě do jedné hodiny od přijetí příkazu k odstranění.

Podle článku 6 nařízení musí adresát zachovat obsah i související údaje, které byly odstraněny nebo k nimž byl znemožněn přístup, po dobu nejméně šesti měsíců, nebo na žádost příslušných orgánů nebo soudů po dobu delší.

Podle čl. 15 odst. 2 nařízení je tento příkaz k odstranění zasílán v jednom z jazyků určených adresátem.

ODDÍL A:

Členský stát vydávajícího příslušného orgánu:

.....

Pozn.: Údaje o vydávajícím příslušném orgánu se uvádějí v oddílech E a F.

Adresát a případně jeho právní zástupce:

.....

Kontaktní místo:

.....

Členský stát, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má bydliště nebo je usazen jeho právní zástupce:

.....

Čas a datum vydání příkazu k odstranění:

.....

Referenční číslo příkazu k odstranění:

.....

ODDÍL B: Teroristický obsah, který má být odstraněn nebo k němuž má být znemožněn přístup ve všech členských státech, a to co nejdříve a v každém případě do jedné hodiny od přijetí příkazu k odstranění:

URL a jakékoli další informace umožňující identifikaci a přesnou lokalizaci teroristického obsahu:

.....

Odůvodnění, proč je materiál považován za teroristický obsah ve smyslu čl. 2 bodu 7 nařízení.

Materiál (zaškrtněte příslušná pole):

☐ podněcuje jiné ke spáchání teroristických trestných činů, například formou glorifikace teroristických činů, nebo obhajuje páchání takových činů (čl. 2 bod 7 písm. a) nařízení)

☐ získává jiné ke spáchání nebo přispění ke spáchání teroristických trestných činů (čl. 2 bod 7 písm. b) nařízení)

☐ získává jiné k účasti na činnostech teroristické skupiny (čl. 2 bod 7 písm. c) nařízení)

☐ poskytuje návod k výrobě nebo použití výbušnin, palných nebo jiných zbraní nebo škodlivých či nebezpečných látek, nebo k jiným specifickým metodám či technikám za účelem spáchání nebo přispění ke spáchání teroristických trestných činů (čl. 2 bod 7 písm. d) nařízení)

☐ vyhrožuje spácháním některého z teroristických trestných činů (čl. 2 bod 7 písm. e) nařízení).

Další informace o důvodech, proč je materiál považován za teroristický obsah:

.....

.....

.....

ODDÍL C: Informace pro poskytovatele obsahu

Upozorňujeme vás, že (v příslušném případě zaškrtněte příslušné pole):

☐ z důvodů veřejné bezpečnosti adresát nesmí informovat poskytovatele obsahu o odstranění teroristického obsahu nebo znemožnění přístupu k němu.

Pokud se toto příslušné pole nepoužije, viz oddíl G pro podrobné informace o možnosti napadnout příkaz k odstranění v členském státě vydávajícího příslušného orgánu podle vnitrostátního práva (kopie příkazu k odstranění musí být na žádost předána poskytovateli obsahu).

ODDÍL D: Informace příslušnému orgánu členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má jeho právní zástupce bydliště nebo je usazen

(Zaškrtněte příslušné pole)

☐ Členský stát, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má jeho právního zástupce bydliště nebo je usazen, je jiný než členský stát vydávajícího příslušného orgánu

☐ Kopie příkazu k odstranění se zasílá příslušnému orgánu členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má jeho právní zástupce bydliště nebo je usazen

ODDÍL E: Údaje o vydávajícím příslušném orgánu

Druh orgánu (zaškrtněte příslušné pole):

☐ soudce, soud nebo vyšetřující soudce

☐ donucovací orgán

☐ jiný příslušný orgán → vyplňte také oddíl F

Údaje o vydávajícím příslušném orgánu nebo jeho zástupci, jenž osvědčuje přesnost a správnost příkazu k odstranění:

Název vydávajícího příslušného orgánu:

.....

Jméno jeho zástupce a pracovní pozice (titul a funkce):

.....

Spis číslo:

.....

Adresa:

.....

Telefon (mezinárodní předvolba) (místní předčíslí):

.....

Fax (mezinárodní předvolba) (místní předčíslí):

.....

E-mailová adresa .....

Datum.....

Úřední razítko (je-li k dispozici) a podpis ([1]):

.....

([1]) Podpis není nutný v případě odeslání příkazu k odstranění ověřenými kanály pro předkládání dokumentů, které mohou zaručit autentičnost příkazu k odstranění obsahu.

ODDÍL F: Kontaktní údaje pro následná opatření

Kontaktní údaje vydávajícího příslušného orgánu pro účely zaslání zpětné vazby ohledně času odstranění obsahu či znemožnění přístupu k němu, nebo pro poskytnutí dalších vysvětlení:

.....

Kontaktní údaje příslušného orgánu členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu nebo v němž má bydliště nebo je usazen jeho právní zástupce:

.....

ODDÍL G: Informace o možných prostředcích nápravy

Informace o příslušném orgánu či soudu, lhůtách a postupech pro napadení příkazu k odstranění:

Příslušný orgán nebo soud, u kterého lze příkaz k odstranění napadnout:

.....

Lhůta pro napadení příkazu k odstranění (dnů/měsíců počínaje od):

.....

Odkaz na ustanovení vnitrostátních právních předpisů:

.....

PŘÍLOHA II

ZPĚTNÁ VAZBA PO ODSTRANĚNÍ TERORISTICKÉHO OBSAHU ČI ZNEMOŽNĚNÍ PŘÍSTUPU K NĚMU

(čl. 3 odst. 6 nařízení Evropského parlamentu a Rady (EU) 2021/784)

ODDÍL A:

Adresát příkazu k odstranění:

.....

Příslušný orgán, který vydal příkaz k odstranění:

.....

Referenční číslo spisu příslušného orgánu, který vydal příkaz k odstranění:

.....

Referenční číslo spisu adresáta:

.....

Čas a datum přijetí příkazu k odstranění:

.....

ODDÍL B:

Opatření přijatá pro splnění příkazu k odstranění (zaškrtněte příslušné pole):

☐ teroristický obsah byl odstraněn

☐ přístup k teroristickému obsahu byl znemožněn ve všech členských státech

Čas a datum přijetí opatření

.....

ODDÍL C: Údaje o adresátovi

Název poskytovatele hostingových služeb

.....

NEBO

jméno/název právního zástupce poskytovatele hostingových služeb:

.....

Členský stát, v němž má poskytovatel hostingových služeb hlavní provozovnu

.....

NEBO

členský stát, v němž má bydliště nebo je usazen právní zástupce poskytovatele hostingových služeb:

.....

Jméno oprávněné osoby:

.....

E-mailová adresa kontaktního místa:

.....

Datum:

.....

PŘÍLOHA III

INFORMACE O NEMOŽNOSTI PROVÉST PŘÍKAZ K ODSTRANĚNÍ

(čl. 3 odst. 7 a 8 nařízení Evropského parlamentu a Rady (EU) 2021/784)

ODDÍL A:

Adresát příkazu k odstranění:

.....

Příslušný orgán, který vydal příkaz k odstranění:

.....

Referenční číslo spisu příslušného orgánu, který vydal příkaz k odstranění:

.....

Referenční číslo spisu adresáta:

.....

Čas a datum přijetí příkazu k odstranění:

.....

ODDÍL B: Neprovedení

1) Příkaz k odstranění nelze provést ve lhůtě z následujících důvodů (zaškrtněte příslušná pole):

☐ vyšší moc nebo faktická nemožnost, za kterou poskytovatel hostingových služeb neodpovídá, včetně objektivně opodstatněných technických nebo provozních důvodů

☐ příkaz k odstranění obsahuje zjevné chyby

☐ příkaz k odstranění neobsahuje dostatečné informace

2) Uveďte další informace týkající se důvodů k neprovedení:

.....

3) Jestliže příkaz k odstranění obsahuje zjevné chyby nebo neobsahuje dostatečné informace, upřesněte, o jaké chyby se jedná a jaké další informace či vysvětlení jsou nezbytné:

.....

ODDÍL C: Údaje o poskytovateli hostingových služeb nebo jeho právním zástupci

Název poskytovatele hostingových služeb

.....

NEBO

jméno/název právního zástupce poskytovatele hostingových služeb:

.....

Jméno oprávněné osoby:

.....

Kontaktní údaje (e-mailová adresa):

.....

Podpis:

.....

Čas a datum:

.....