Rada
Evropské unie

Brusel 14. září 2018
(OR. en)

12129/18

Interinstitucionální spis:
2018/0331 (COD)

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

NÁVRH

Odesílatel:	Jordi AYET PUIGARNAU, ředitel, za generálního tajemníka Evropské komise
Datum přijetí:	12. září 2018
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	COM(2018) 640 final
Předmět:	Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o prevenci šíření teroristického obsahu online *Příspěvek Evropské komise k zasedání vedoucích představitelů v Salcburku ve dnech 19.–20. září 2018*

Delegace naleznou v příloze dokument COM(2018) 640 final.

Příloha: COM(2018) 640 final

EVROPSKÁ
KOMISE

V Bruselu dne 12.9.2018
COM(2018) 640 final

2018/0331 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o prevenci šíření teroristického obsahu online

Příspěvek Evropské komise k zasedání vedoucích představitelů v Salcburku ve dnech 19.–20. září 2018

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

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

1.1. Odůvodnění a cíle návrhu

Díky všudypřítomnosti internetu mohou jeho uživatele komunikovat, pracovat, společensky žít, tvořit, získávat informace a obsahy a sdílet je se stovkami milionů jedinců na celé planetě. Internetové platformy významně zlepšují ekonomické a sociální podmínky uživatelů v Unii i za jejími hranicemi. Možnost oslovit tak velké publikum za minimální náklady ale také přitahuje zločince, kteří chtějí internet zneužívat k nezákonným účelům. Nedávné teroristické útoky na půdě EU ukázaly, jak teroristé zneužívají internet k získávání a náboru stoupenců, k přípravě teroristické činnosti či jejímu napomáhání, ke glorifikaci hrůzných teroristických činů a k vyzývání ostatních, aby se připojili a rozsévali strach u široké veřejnosti.

Teroristické obsahy sdílené online za takovým účelem jsou šířeny prostřednictvím poskytovatelů hostingových služeb, kteří umožňují nahrávání obsahu od třetích stran. Je prokázáno, že teroristické obsahy online napomáhají radikalizaci a že inspirovaly útoky tzv. „osamělých vlků“ v případě několika nedávných teroristických útoků v Evropě. Takové obsahy nejenže mají výrazně negativní dopad na jedince a společnost jako celek, ale také snižují důvěru uživatelů v internet a negativně poznamenávají obchodní modely a dobré jméno dotčených společností. Teroristé nezneužívají pouze velké platformy sociálních médií, ale ve stále větší míře také služby menších poskytovatelů, kteří nabízejí různé druhy hostingových služeb na celém světě. Takové případy zneužívání internetu především zdůrazňují společenskou odpovědnost internetových platforem, které mají povinnost chránit své uživatele před teroristickými obsahy a závažnými ohroženími bezpečnosti, jež tyto obsahy představují pro společnost jako celek.

Poskytovatelé hostingových služeb v reakci na naléhání ze strany veřejných orgánů zavedli určitá opatření k potírání teroristických obsahů v rámci svých služeb. Dosáhlo se jistých úspěchů prostřednictvím dobrovolných rámců a partnerství, včetně internetového fóra EU, které bylo zahájeno v prosinci 2015 jako součást Evropského programu pro bezpečnost. Internetové fórum EU prosazovalo dobrovolnou spolupráci a činnost členských států a poskytovatelů hostingových služeb s cílem snížit dostupnost teroristických obsahů online a posílit postavení partnerů občanské společnosti, aby se rozšířila účinná protiargumentace na internetu. Tyto snahy přispěly k hlubší spolupráci, zlepšení odezvy ze strany společností na hlášení zasílaná vnitrostátními orgány, jakož i jednotkou Europolu pro oznamování internetového obsahu, k využití dobrovolných proaktivních opatření ke zlepšení automatizovaného odhalování teroristického obsahu, intenzivnější spolupráci mezi podniky, včetně vývoje „databáze hashů“ s cílem zabránit nahrávání známého teroristického obsahu na propojené platformy, jakož i ke zvýšení transparentnosti veškerého úsilí v tomto směru. Spolupráce v rámci internetového fóra EU by sice měla i v budoucnosti pokračovat, avšak dobrovolná řešení ukázala své limity. Za prvé – ne všichni postižení poskytovatelé hostingových služeb se do fóra zapojili a – za druhé – rozsah a tempo úspěšné činnosti ze strany poskytovatelů hostingových služeb jako celku nepostačují k účinnému řešení příslušného problému.

Vzhledem k těmto omezením je zřejmé, že bude zapotřebí posílit činnost Evropské unie zaměřenou proti teroristickému obsahu na internetu. Komise dne 1. března 2018 přijala doporučení o opatřeních pro efektivní boj proti nezákonnému obsahu online, které navazuje

na sdělení Komise ze září[1], jakož i na snahy v rámci internetového fóra EU. Doporučení obsahuje zvláštní kapitolu, v níž je vymezena řada opatření s cílem účinně zamezit nahrávání a sdílení teroristické propagandy online, k nimž patří zlepšení procesu oznamování, hodinová časová lhůta pro reakci na hlášení, proaktivnější zjišťování, účinnější odstraňování a dostatečné záruky pro přesné posouzení teroristického obsahu[2].

Potřebu posílit činnost zaměřenou na potírání teroristického obsahu online odrážely rovněž výzvy ze strany členských států EU a některé státy již v této věci přijaly právní předpisy nebo vyjádřily svůj úmysl tak učinit. V návaznosti na sérii teroristických útoků, k nimž v EU došlo, a vzhledem ke skutečnosti, že teroristický obsah online je i nadále snadno dostupný, Evropská rada ve dnech 22.–23. června 2017 vyzvala podniky k tomu, aby vyvinuly „nové technologie a nástroje ke zlepšení automatického odhalování a odstraňování obsahu, jenž podněcuje k teroristickým činům. V nezbytných případech by toto úsilí mělo být doplněno příslušnými legislativními opatřeními na úrovni EU“. Evropská rada dne 28. června 2018 uvítala „záměr Komise předložit legislativní návrh v zájmu zlepšení odhalování a odstraňování obsahu, jenž podněcuje k nenávisti a k páchání teroristických činů.“ Evropský parlament dále ve svém usnesení o online platformách a jednotném digitálním trhu ze dne 15. června 2017 vyzval dotyčné platformy k tomu, aby „zintenzivnily opatření pro boj proti nezákonnému a škodlivému obsahu“, a zároveň vyzval Komisi, aby předložila návrhy řešení.

Komise chce uvedené problémy řešit a reagovat na výzvy členských států a Evropského parlamentu. Proto si v tomto návrhu klade za cíl zavést jasný a harmonizovaný právní rámec pro prevenci zneužívání hostingových služeb k šíření teroristického obsahu online, aby se zaručilo hladké fungování jednotného digitálního trhu a současně se zajistila důvěra a bezpečnost. Cílem tohoto nařízení je vyjasnit otázku odpovědnosti poskytovatelů hostingových služeb při přijímání veškerých vhodných, rozumných a přiměřených opatření nezbytných k zajištění bezpečnosti jejich služeb a k rychlému a účinnému odhalení a odstranění teroristického obsahu online za současného zohlednění zásadního významu svobody projevu a informací v otevřené demokratické společnosti. Rovněž zavádí řadu nezbytných záruk určených k zajištění plného dodržování základních práv, jako je svoboda projevu a informací v demokratické společnosti, vedle možností soudní nápravy, kterou zaručuje právo na účinnou právní ochranu zakotvené v článku 19 SEU a v článku 47 Listiny základních práv Evropské unie.

Stanovením minimálního souboru povinností náležité péče pro poskytovatele hostingových služeb, který bude zahrnovat zvláštní pravidla a úkoly, jakož i povinností pro členské státy, si návrh klade za cíl zvýšit účinnost současných opatření pro odhalování, identifikaci a odstraňování teroristického obsahu online, aniž by zasahoval do základních práv, jako je svoboda projevu a informací. Takový harmonizovaný právní rámec usnadní poskytování služeb online v rámci jednotného digitálního trhu, zaručí rovné podmínky pro všechny poskytovatele hostingových služeb, kteří své služby orientují na Evropskou unii, a poskytne solidní právní rámec pro odhalování a odstraňování teroristického obsahu a současně i náležité záruky ochrany základních práv. Povinnosti týkající se transparentnosti konkrétně zvýší důvěru mezi občany a zejména mezi uživateli internetu a posílí odpovědnost a transparentnost činností jednotlivých společností, a to i ve vztahu k veřejným orgánům. Návrh také stanoví povinnost zavést nápravná opatření a mechanismy pro podávání stížností, které uživatelům zajistí, že budou moci napadnout odstranění svého obsahu. Povinnosti uložené

[1] Sdělení (COM(2017) 555 final) o boji proti nezákonnému obsahu online.

[2] Doporučení (C(2018) 1177 final) ze dne 1. března 2018 o opatřeních pro efektivní boj proti nezákonnému obsahu online.

členským státům přispějí k dosažení těchto cílů a také zlepší schopnost příslušných orgánů přijímat vhodnáh opatření proti teroristickému obsahu online a bojovat proti zločinu. V případě, že poskytovatelé hostingových služeb nebudou nařízení dodržovat, mohou členské státy uložit sankce.

1.2 Soulad s platným právním rámcem EU v této oblasti politiky

Přítomný návrh je v souladu s *acquis* v oblasti jednotného digitálního trhu a obzvlášť se směrnicí o elektronickém obchodu. Zejména by žádná opatření, která poskytovatel hostingových služeb přijme v souladu s tímto nařízením, včetně jakýchkoli proaktivních opatření, neměla sama o sobě vést k tomu, že by poskytovatel služeb ztratil možnost využít výjimku z odpovědnosti stanovenou v rámci určitých podmínek v článku 14 směrnice o elektronickém obchodu. Rozhodnutí vnitrostátních orgánů o uložení přiměřených a zvláštních proaktivních opatření by ze zásady nemělo vést k uložení obecné povinnosti dohledu, jak je s ohledem na členské státy definována v čl. 15 odst. 1 směrnice 2000/31/ES. Nicméně vzhledem k obzvláště závažným rizikům spojeným se šířením teroristických obsahů se mohou rozhodnutí podle tohoto nařízení od této zásady v rámci EU výjimečně odchylovat. Příslušný orgán musí před přijetím takových rozhodnutí dosáhnout vhodné rovnováhy mezi potřebami veřejné bezpečnosti a dotčenými zájmy a základními právy, kam patří zejména svoboda projevu a informací, svoboda podnikání a ochrana osobních údajů a soukromí. Povinnosti náležité péče ukládané poskytovatelům hostingových služeb by tuto rovnováhu, která je vyjádřena ve směrnici o elektronickém obchodu, měly odrážet a respektovat.

Návrh je rovněž v souladu a úzce sladěn se směrnicí (EU) 2017/541 o boji proti terorismu, jejímž cílem je harmonizovat právní předpisy členských států, jež kriminalizují teroristické trestné činy. Článek 21 směrnice o boji proti terorismu požaduje, aby členské státy přijaly opatření, která zajistí rychlé odstranění online obsahu omezeného na veřejné podněcování a umožní členským státům volbu opatření. Toto nařízení se vzhledem ke své preventivní povaze vztahuje nejen na materiál podněcující terorismus, ale také na materiál pro účely náboru či odborné přípravy, což odráží jiné trestné činy související s teroristickými činnostmi, které směrnice 2017/541/EU rovněž upravuje. Toto nařízení poskytovatelům hostingových služeb přímo ukládá povinnosti náležité péče spočívající v odstraňování teroristického obsahu a harmonizuje postupy pro vydávání příkazů k odstranění s cílem omezit přístup k teroristickému obsahu online.

Nařízení doplňuje pravidla stanovená v budoucí směrnici o audiovizuálních mediálních službách, jelikož jeho osobní a věcná oblast působnosti jsou širší. Nařízení se nevztahuje pouze na platformy pro sdílení videa, ale na všechny různé druhy hostingových služeb. Navíc zahrnuje nejen videa, ale také obrázky a text. Toto nařízení navíc přesahuje – v oblasti hmotněprávních ustanovení – rámec směrnice tím, že harmonizuje pravidla, která se týkají proaktivních opatření a žádostí o odstranění teroristického obsahu.

Navrhované nařízení vychází z doporučení Komise[3] o nezákonném obsahu z března 2018. Uvedené doporučení zůstává v platnosti a všechny osoby, které se podílejí na snižování dostupnosti nezákonného obsahu – včetně teroristického obsahu –, by měly nadále společně usilovat o provádění opatření stanovených v doporučení.

[3] Doporučení (C(2018) 1177 final) ze dne 1. března 2018 o opatřeních pro efektivní boj proti nezákonnému obsahu online.

1.3 Shrnutí navrhovaného nařízení

Osobní působnost návrhu zahrnuje poskytovatele hostingových služeb, kteří nabízejí své služby v rámci Unie, bez ohledu na místo usazení nebo jejich velikost. Navrhované právní předpisy zavádějí řadu opatření, která mají zabránit zneužívání hostingových služeb k šíření teroristického obsahu na internetu, aby se zaručilo hladké fungování jednotného digitálního trhu a zároveň se zajistila důvěra a bezpečnost. Definice nezákonného teroristického obsahu je v souladu s definicí teroristických trestných činů, jak je stanovena ve směrnici (EU) 2017/541, kde je tento obsah definován jako informace, které jsou využívány k podněcování a glorifikaci páchání teroristických trestných činů, k podpoře teroristických trestných činů a k poskytování pokynů k páchání teroristických trestných činů, jakož i k podpoře účasti v teroristických skupinách.

Aby se zajistilo odstranění nezákonného teroristického obsahu, zavádí nařízení příkaz k odstranění, který může být vydán jako správní nebo soudní rozhodnutí příslušným orgánem v členském státě. V takových případech je poskytovatel hostingových služeb povinen do jedné hodiny obsah odstranit nebo k němu znemožnit přístup. Nařízení navíc harmonizuje minimální požadavky na hlášení zaslaná příslušnými orgány členských států a orgány Unie (jako je Europol) poskytovatelům hostingových služeb, která mají být posouzena na základě jejich příslušných podmínek. A konečně, nařízení vyžaduje, aby poskytovatelé hostingových služeb tam, kde je to vhodné, přijali proaktivní opatření úměrná úrovni rizika a odstraňovali teroristický materiál ze svých služeb, včetně zavádění nástrojů pro jeho automatické odhalování.

Opatření určená k redukci teroristického obsahu na internetu jsou spojena s řadou klíčových záruk zajišťujících úplnou ochranu základních práv. V rámci opatření na ochranu obsahu, který není teroristický, před chybným odstraněním, návrh stanoví povinnost zavést nápravné mechanismy a mechanismy pro podávání a vyřizování stížností, aby se zajistilo, že uživatelé budou moci odstranění svého obsahu napadnout. Kromě toho nařízení zavádí povinnosti týkající se transparentnosti opatření, která jsou přijata proti teroristickému obsahu, poskytovateli služeb, a tím zajišťuje odpovědnost vůči uživatelům, občanům a veřejným orgánům.

Nařízení rovněž ukládá členským státům povinnost zajistit, aby jejich příslušné orgány měly nezbytnou kapacitu pro zásah proti teroristickému obsahu na internetu. Kromě toho jsou členské státy povinny vzájemně se informovat a spolupracovat a mohou využívat kanály zřízené Europolem s cílem zajistit koordinaci, pokud jde o příkazy k odstranění a hlášení. Nařízení rovněž stanoví povinnosti poskytovatelů hostingových služeb podávat podrobné zprávy o přijatých opatřeních a informovat donucovací orgány při odhalení obsahu, který ohrožuje život nebo bezpečnost. A v neposlední řadě jsou poskytovatelé hostingových služeb povinni uchovávat obsah, který odstraňují, což funguje jako záruka proti chybnému odstranění a zajišťuje zachování případných důkazů pro účely prevence, odhalování, vyšetřování a stíhání teroristických trestných činů.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

2.1 Právní základ

Právním základem je článek 114 Smlouvy o fungování Evropské unie, který stanoví zavedení opatření k zajištění fungování vnitřního trhu.

Článek 114 představuje vhodný právní základ pro harmonizaci podmínek pro poskytovatele hostingových služeb při poskytování přeshraničních služeb v rámci jednotného digitálního trhu a pro řešení rozdílů mezi ustanoveními jednotlivých členských států, které by jinak

mohly fungování vnitřního trhu bránit. Rovněž zabraňuje vzniku budoucích překážek hospodářské činnosti v důsledku rozdílů ve vývoji vnitrostátních právních předpisů.

Článek 114 SFEU lze rovněž použít k ukládání povinností poskytovatelům hostingových služeb usazeným mimo území EU, jestliže jejich poskytování služeb ovlivňuje vnitřní trh, neboť to je nezbytné pro dosažení kýženého cíle souvisejícího s vnitřním trhem.

2.2 Volba nástroje

Ustanovení článku 114 SFEU dává normotvůrci Unie možnost přijímat nařízení a směrnice.

Vzhledem k tomu, že se návrh týká povinností poskytovatelů služeb, kteří obvykle nabízejí své služby ve více než jednom členském státě, by rozdílné uplatňování těchto pravidel bránilo v poskytování služeb poskytovateli působícími v několika členských státech. Nařízení umožňuje, aby stejná povinnost byla v celé Unii uložena jednotným způsobem, byla přímo použitelná, zajišťovala jasnost a větší právní jistotu a zabraňovala rozdílnému provádění v členských státech. Z těchto důvodů se za nejvhodnější formu použití tohoto nástroje považuje nařízení.

2.3 Subsidiarita

Vzhledem k přeshraničnímu rozměru řešených problémů musí být opatření zahrnutá do návrhu přijata na úrovni Unie, aby mohlo být dosaženo příslušných cílů. Internet je svou povahou přeshraniční a obsah uložený v jednom členském státě je běžně přístupný z jakéhokoli jiného členského státu.

Dochází k roztříštěnosti rámce vnitrostátních pravidel pro boj proti teroristickému obsahu online a rizika se zvyšují. To by vedlo k zátěži pro společnosti, které by musely dodržovat odlišné právní předpisy, a také by tímvznikly nerovné podmínky pro společnosti, jakož i bezpečnostní mezery.

Opatření na úrovni EU proto zvyšuje právní jistotu a zvyšuje efektivitu kroků ze strany poskytovatelů hostingových služeb proti teroristickému obsahu na internetu. Více společností – včetně společností usazených mimo Evropskou unii – by tak mohlo podniknout příslušné kroky, což by posílilo integritu jednotného digitálního trhu.

To odůvodňuje potřebu opatření na úrovni EU, jak bylo uvedeno v závěrech Evropské rady z června 2018, v nichž je Komise vyzvána k tomu, aby v této oblasti předložila legislativní návrh.

2.4 Proporcionalita

Návrh stanoví pravidla pro poskytovatele hostingových služeb, kteří mají uplatňovat opatření k rychlému odstranění teroristického obsahu ze svých služeb. Klíčové prvky tento návrh omezují pouze na to, co je nezbytné k dosažení cílů politiky.

Návrh zohledňuje zátěž pro poskytovatele hostingových služeb a záruky, včetně ochrany svobody projevu a informací, jakož i dalších základních práv. Časová lhůta jedné hodiny pro odstranění se vztahuje pouze na příkazy k odstranění, u kterých příslušné orgány stanovily nezákonnost v rozhodnutí, které podléhá soudnímu přezkumu. V případě hlášení existuje povinnost zavést opatření usnadňující rychlé posouzení teroristického obsahu, nezavádí se však povinnost tento obsah odstranit ani absolutní lhůty. Konečné rozhodnutí zůstává dobrovolným rozhodnutím poskytovatele hostingových služeb. Zátěž společností spojenou s posouzením obsahu zmírňuje skutečnost, že příslušné orgány členských států a Unie poskytují vysvětlení toho, proč může být obsah považován za teroristický. Poskytovatelé hostingových služeb v případě potřeby přijmou proaktivní opatření na ochranu svých služeb

proti šíření teroristického obsahu. Specifické povinnosti týkající se proaktivních opatření se vztahují pouze na ty poskytovatele hostitelských služeb, kteří jsou vystaveni teroristickému obsahu, což dokládá přijetí příkazu k odstranění, který nabyl právní moci, a měly by být přiměřené úrovni rizika a zdrojům společnosti. Uchování odstraněného obsahu a souvisejících údajů se omezuje na dobu přiměřenou účelu, jímž je umožnit řízení správního nebo soudního přezkumu, a pro účely prevence, odhalování, vyšetřování a stíhání teroristických trestných činů.

3. VÝSLEDKY HODNOCENÍ EX POST, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

3. 1. Konzultace se zúčastněnými stranami

Během přípravy tohoto legislativního návrhu Komise konzultovala všechny relevantní zúčastněné strany, aby pochopila jejich názory a možný budoucí postup. Komise realizovala otevřenou veřejnou konzultaci týkající se opatření za účelem zlepšení účinnosti boje proti nezákonnému obsahu, přičemž obdržela 8 961 odpovědí, z nichž 8 749 pocházelo od jednotlivců, 172 od organizací, 10 od veřejné správy a 30 od jiných kategorií respondentů. Současně byl u náhodného vzorku 33 500 obyvatel EU proveden průzkum Eurobarometr týkající se nezákonného obsahu online. Během května a června 2018 Komise ohledně konkrétních opatření pro boj proti teroristickému obsahu na internetu konzultovala také orgány členských států a poskytovatele hostingových služeb.

Většina zúčastněných stran v podstatě uvedla, že teroristický obsah na internetu představuje závažný celospolečenský problém, který ovlivňuje uživatele internetu a obchodní modely poskytovatelů hostingových služeb. Obecněji řečeno, 65 % respondentů průzkumu Eurobarometr[4] se domnívalo, že internet není pro uživatele bezpečný, a 90 % respondentů považuje za důležité omezovat šíření nezákonného obsahu online. Konzultace se členskými státy ukázaly, že přestože dobrovolná ujednání určité výsledky přinášejí, velká skupina vnímá nutnost závazných povinností týkajících se teroristického obsahu. Tento názor se odráží také v závěrech Evropské rady z června 2018. Ačkoliv byli poskytovatelé hostingových služeb nakloněni pokračování dobrovolných opatření, uvědomovali si potenciálně negativní vliv vznikající právní nesourodosti v Unii.

Mnoho zúčastněných stran rovněž upozornilo na potřebu zajistit, aby byla regulační opatření zaměřená na odstraňování obsahu, a to obzvláště proaktivní opatření a striktní harmonogramy, v rovnováze s ochrannými opatřeními zajišťujícími základní práva, zejména svobodu projevu. Zúčastněné strany uvedly několik nezbytných opatření vztahujících se k transparentnosti, odpovědnosti a také nutnosti lidské kontroly při nasazení automatizovaných nástrojů.

3. 2. Posouzení dopadů

Výbor pro kontrolu regulace vydal k posouzení dopadů kladné stanovisko s výhradami a připojil několik návrhů na zlepšení[5]. V návaznosti na toto stanovisko byla zpráva o posouzení dopadů doplněna tak, aby řešila hlavní připomínky Výboru, zaměřila se konkrétně na teroristický obsah a současně zdůraznila důsledky ve vztahu k fungování jednotného digitálního trhu a zahrnovala také hlubší analýzu dopadů na základní práva a fungování záruk navrhovaných v jednotlivých v možnostech.

---

4 Průzkum Eurobarometr 469, Nezákonný obsah online, červen 2018.

5 Odkaz na stanovisko Výboru pro kontrolu regulace v Rejstříku dokumentů.

Pokud by nebyla přijata další opatření, předpokládá se pokračování dobrovolné činnosti podle základního scénáře a její určitý vliv na omezování teroristického obsahu online. Nicméně nelze předpokládat, že budou dobrovolná opatření uplatňovat všichni poskytovatelé hostingových služeb vystavení takovému obsahu. Lze očekávat prohloubení právní nesourodosti, které povede k dalším překážkám na poli poskytování přeshraničních služeb. Kromě základního scénáře byly zvažovány tři hlavní možnosti politiky s rostoucí mírou účinnosti, pokud jde o plnění cílů stanovených v posouzení dopadů a celkového politického cíle omezení teroristického obsahu online.

Rozsah těchto povinností ve všech třech možnostech se zaměřoval na všechny poskytovatele hostingových služeb (osobní působnost) usazené v EU a ve třetích zemích, pokud nabízejí služby v Unii (místní působnost). S ohledem na povahu problematiky a nutnost zabránit zneužívání menších platforem se v žádné z možností nepředpokládají výjimky pro malé a střední podniky. Všechny možnosti by vyžadovaly, aby poskytovatelé hostingových služeb za účelem zajištění vykonavatelnosti pravidel EU stanovili zákonného zástupce v EU, a to včetně společností usazených mimo EU. Všechny možnosti předpokládaly, že členské státy vytvoří mechanismy sankcí.

Všechny možnosti zahrnovaly plán vytvoření nového, harmonizovaného systému právních příkazů k odstranění obsahu, které by se vztahovaly na teroristický obsah online a které by vydávaly vnitrostátní orgány poskytovatelům hostingových služeb, a také požadavek na odstranění obsahu do jedné hodiny. Tyto příkazy by nemusely nutně vyžadovat posouzení ze strany poskytovatele hostingových služeb a podléhaly by soudní nápravě.

Společnými znaky všech tří možností jsou ochranná opatření, zejména postupy řešení stížností, účinná nápravná opatření včetně soudní nápravy a další ustanovení za účelem prevence chybného odstranění obsahu, který není teroristický, a zajištění souladu se základními právy. Všechny možnosti navíc zahrnují oznamovací povinnosti ve formě veřejné transparentnosti a podávání zpráv členským státům a Komisi, ale také příslušným orgánům v případě podezření na spáchání trestného činu. Navíc se předpokládá zavedení povinností spolupráce mezi vnitrostátními orgány, poskytovateli hostingových služeb a případně Europolem.

Hlavní rozdíly mezi těmito třemi možnostmi spočívají v rozsahu vymezení teroristického obsahu, míře harmonizace hlášení, rozsahu proaktivních opatření, koordinaci povinností u členských států a také požadavcích na uchovávání údajů. Možnost 1 by omezovala věcnou působnost na obsah šířený za účelem přímého podněcování ke spáchání teroristického činu dle úzké definice, zatímco možnosti 2 a 3 by uplatňovaly komplexnější přístup a zahrnovaly také materiál týkající se náboru a výcviku. U proaktivních opatření by v rámci možnosti 1 poskytovatelé hostingových služeb vystavení teroristickému obsahu museli provádět posouzení rizik, ale proaktivní opatření, která by rizika řešila, by byla i nadále dobrovolná. Možnost 2 by od poskytovatelů hostingových služeb vyžadovala, aby sestavili akční plán, který by mohl zahrnovat nasazení automatizovaných nástrojů prevence opětovného nahrávání obsahu, který již byl odstraněn. Možnost 3 zahrnuje komplexnější proaktivní opatření, která by od poskytovatelů služeb vystavených teroristickému obsahu vyžadovala také identifikaci nového materiálu. Ve všech možnostech by byly požadavky vztahující se na proaktivní opatření úměrná úrovni expozice teroristickému materiálu a také ekonomickým možnostem poskytovatele služeb. Co se týče hlášení, možnost 1 by neharmonizovala přístup k hlášením, zatímco možnost 2 by tak činila ve vztahu k Europolu a možnost 3 by navíc zahrnovala také hlášení ze strany členských států. V rámci možností 2 a 3 by byly členské státy povinny se vzájemně informovat, koordinovat svou činnost a spolupracovat, přičemž v rámci možnosti 3 by musely navíc zajistit, aby byly jejich příslušné orgány schopny odhalovat a oznamovat

teroristický obsah. A konečně možnost 3 také zahrnuje požadavek uchovávat údaje pro případ chybného odstranění a pro účely vyšetřování trestné činnosti.

Kromě právní úpravy se u všech legislativních možností předpokládalo, že budou doprovázeny řadou podpůrných opatření, jejichž účelem bude zejména zajistit spolupráci mezi vnitrostátními orgány a Europolem, součinnost s poskytovateli hostingových služeb a také podporu výzkumu, vývoje a inovací v oblasti vývoje a zavádění technologických řešení. Po přijetí takového právního nástroje lze pro malé a střední podniky zavádět také další podpůrné nástroje a nástroje zaměřené na zvyšování informovanosti.

Z posouzení dopadů vyplývá, že pro realizaci politického cíle bude zapotřebí několik opatření. Vhodnější než úzká definice obsahu (možnost 1) by bylo komplexní vymezení teroristického obsahu, které by podchytilo nejškodlivější materiál. Proaktivní povinnosti omezené na prevenci opětovného nahrání teroristického obsahu (možnost 2) by byly ve srovnání s povinnostmi souvisejícími s odhalováním nového teroristického obsahu (možnost 3) méně účinné. Ustanovení týkající se hlášení by měla zahrnovat hlášení ze strany Europolu i členských států (možnost 3) a neměla by se omezovat pouze na hlášení ze strany Europolu (možnost 2), protože hlášení ze strany členských států je důležitou součástí celkového úsilí zaměřeného na omezení dostupnosti teroristického obsahu online. Taková opatření by bylo nutné provést spolu s opatřeními, která jsou všem třem možnostem společná, a to včetně efektivních opatření zajišťujících prevenci chybného odstranění obsahu.

3. 3. Základní práva

Teroristická propaganda na internetu se snaží podněcovat jednotlivce k páchání teroristických útoků, a to včetně poskytování podrobných pokynů, jak způsobit maximální újmu. Další propaganda se obvykle šíří po těchto zrůdných činech, kdy jsou takové činy glorifikovány a ostatní jsou povzbuzováni, aby následovali jejich příkladu. Toto nařízení přispívá k ochraně veřejné bezpečnosti snížením dostupnosti teroristického obsahu, který propaguje a nabádá k porušování základních práv.

Návrh by potenciálně mohl mít dopad na řadu základních práv:

a) práva poskytovatelů obsahu: právo na svobodu projevu, právo na ochranu osobních údajů, právo na respektování soukromého a rodinného života, zásada zákazu diskriminace a právo na účinnou právní ochranu,

b) práva poskytovatelů služeb: právo na svobodu podnikání, právo na účinnou právní ochranu,

c) práva všech občanů: a právo na svobodu projevu a informací.

S ohledem na příslušné *acquis* jsou do navrhovaného nařízení zahrnuty náležité a efektivní záruky s cílem zajistit ochranu práv těchto osob.

V tomto kontextu je prvním prvkem skutečnost, že nařízení stanoví definici teroristického obsahu online v souladu s definicí teroristických trestných činů uvedenou ve směrnici (EU) 2017/541. Tato definice se vztahuje na příkazy k odstranění obsahu a hlášení, ale také na proaktivní opatření. Definice zajišťuje, že bude odstraňován pouze nezákonný obsah, který odpovídá celounijní definici souvisejících trestných činů. Kromě toho nařízení obsahuje obecnou povinnost náležité péče poskytovatelů hostingových služeb, která jim ukládá jednat ohledně uchovávaného obsahu s řádnou péčí, přiměřeně a nediskriminačním způsobem, a to zejména při uplatňování jejich vlastních podmínek s cílem zabránit odstranění obsahu, který není teroristickým obsahem.

Konkrétněji vzato, nařízení je koncipováno tak, aby zajistilo proporcionalitu realizovaných opatření ve vztahu k základním právům. Pokud jde o příkazy k odstranění obsahu, posouzení obsahu (včetně případné právní kontroly) příslušnými orgány odůvodňuje u tohoto opatření hodinový časový limit na odstranění obsahu. Navíc ustanovení tohoto nařízení, která se vztahují na hlášení, se omezují pouze na hlášení odeslaná příslušnými orgány a orgány Unie s uvedením důvodů, proč by mohl být obsah považován za teroristický. Přestože odpovědnost za odstranění obsahu označeného v hlášení leží na poskytovateli hostingových služeb, rozhodnutí je zprostředkováno výše uvedeným posouzením.

U proaktivních opatření leží zodpovědnost za identifikaci, posouzení a odstranění obsahu na poskytovatelích hostingových služeb, kteří mají povinnost zavést ochranná opatření za účelem prevence chybného odstraňování obsahu, včetně nástrojů lidské kontroly, a to zejména v případě, kdy je třeba posoudit jeho kontext. Navíc, na rozdíl od základního scénáře, kdy nejvíce dotčené společnosti zavádějí automatizované nástroje bez veřejného dohledu, podléhá návrh těchto opatření a jejich provedení oznamovací povinnosti vůči příslušným orgánům ve členských státech. Tato povinnost zmírňuje rizika chybného odstraňování u společností zavádějících nové nástroje i u těch, které je již využívají. Kromě toho mají poskytovatelé hostingových služeb povinnost poskytovat poskytovatelům obsahu uživatelsky vstřícné mechanismy pro podání stížností, aby měli možnost zpochybnit rozhodnutí o odstranění jejich obsahu a zpřístupňovat široké veřejnosti zprávy o transparentnosti.

Pokud by navzdory těmto ochranným opatřením došlo k chybnému odstranění obsahu a souvisejících údajů, je povinností poskytovatelů hostingových služeb takové údaje uchovávat po dobu šesti měsíců, aby je bylo možné obnovit pro účely zajištění účinnosti postupů v oblasti řešení stížností a kontroly s ohledem na ochranu svobody projevu a informací. Uchovávání údajů je současně prospěšné také z hlediska prosazování práva. Poskytovatelé hostingových služeb musí zavést technická a organizační ochranná opatření, aby zajistili, že údaje nebudou využity pro jiné účely.

Navrhovaná opatření, zejména opatření související s příkazy k odstranění obsahu, hlášeními, proaktivními opatřeními a uchováváním údajů by měla nejen chránit uživatele internetu před teroristickým obsahem, ale také prostřednictvím omezování dostupnosti teroristického obsahu online přispívat k ochraně práva občanů na život.

4. ROZPOČTOVÉ DŮSLEDKY

Legislativní návrh nařízení nemá dopad na rozpočet Unie.

5. OSTATNÍ PRVKY

5. 1. Plány provádění a způsob monitorování, hodnocení a podávání zpráv

Komise stanoví [do jednoho roku od data použitelnosti tohoto nařízení] podrobný program monitorování výstupů, výsledků a dopadů tohoto nařízení. Program monitorování stanoví ukazatele, prostředky a intervaly shromažďování údajů a dalších potřebných důkazů. Specifikuje opatření, která mají být přijata Komisí a členskými státy při shromažďování a analýze údajů a dalších důkazů za účelem monitorování pokroků a hodnocení nařízení.

Na základě zavedeného monitorovacího programu Komise podá do dvou let od okamžiku, kdy toto nařízení vstoupí v platnost, zprávu o provedení tohoto nařízení, která se bude opírat o zprávy o transparentnosti zveřejněné společnostmi a také informace poskytnuté členskými

státy. Komise provede hodnocení tohoto nařízení až po čtyřech letech od okamžiku, kdy nařízení vstoupí v platnost.

Na základě zjištění vyplývajících z hodnocení, včetně stanoviska, zda nařízení vykazuje určité nedostatky či slabé stránky, a s ohledem na technický vývoj posoudí Komise nutnost rozšířit oblast působnosti nařízení. V případě potřeby předloží Komise návrhy úprav tohoto nařízení.

Komise zajistí podporu provádění, monitorování a hodnocení nařízení prostřednictvím skupiny odborníků Komise. Tato skupina bude také zajišťovat spolupráci mezi poskytovateli hostingových služeb, donucovacími orgány a Europolem; pěstovat komunikaci a postupy pro účely odhalování a odstraňování teroristického obsahu, poskytovat své doborné znalosti vývoje způsobů působení teroristů na internetu; v příslušných případech poskytovat poradenství a vedení, aby bylo možné ustanovení plnit.

Provádění navrhovaného nařízení lze podpořit prostřednictvím různých podpůrných opatření. Mezi ně patří možný vývoj platformy v rámci Europolu, která by přispívala ke koordinaci hlášení a příkazů k odstranění obsahu. Výzkum vývoje způsobů teroristického působení financovaný Evropskou unií zlepšuje porozumění a informovanost všech příslušných zúčastněných stran. Program Horizont 2020 navíc podporuje výzkum za účelem vývoje nových technologií, a to včetně automatizované prevence nahrávání teroristického obsahu. Komise bude pokračovat v analýzách, jak podporovat příslušné orgány a poskytovatele hostingových služeb při provádění tohoto nařízení prostřednictvím finančních nástrojů EU.

5. 2. Podrobné vysvětlení konkrétních ustanovení návrhu

Článek 1 vymezí předmět nařízení a uvádí, že nařízení stanoví pravidla prevence zneužívání hostingových služeb k šíření teroristického obsahu online, a to včetně uložení povinnosti náležité péče poskytovatelům hostingových služeb a opatření, která musí zavést členské státy. Stanoví také místní působnost, přičemž zahrnuje poskytovatele hostingových služeb nabízející služby v Unii, a to bez ohledu na jejich provozovnu.

Článek 2 uvádí definice pojmů použitých v návrhu. Stanoví také definici teroristického obsahu pro preventivní účely, přičemž čerpá ze směrnice o boji proti terorismu, aby postihla materiál a informace, které podněcují, nabádají a obhajují páchání či podílení se na teroristických trestných činech, uvádějí pokyny k páchání takových trestných činů nebo propagují účast na činnostech teroristické skupiny.

Článek 3 stanoví povinnosti náležité péče, které mají být plněny poskytovateli hostingových služeb při jednání v souladu s tímto nařízením a zejména s ohledem na dotčená základní práva. Stanoví náležitá ustanovení, která je nutné zanést do podmínek poskytovatelů hostingových služeb a poté zajistit jejich uplatňování.

Článek 4 stanoví požadavky vůči členským státům, aby příslušným orgánům udělily pravomoci vydávat příkazy k odstranění obsahu, a stanoví požadavek, aby poskytovatelé hostingových služeb odstranili obsah do jedné hodiny od přijetí příkazu k odstranění obsahu. Stanoví také minimální náležitosti příkazů k odstranění obsahu, postupy pro poskytovatele hostingových služeb při předávání zpětné vazby vydávajícím orgánům a povinnost informovat takový orgán v případě, že nelze příkaz provést nebo je-li zapotřebí bližších podrobností. Vydávajícímu orgánu ukládá povinnost informovat orgán dohlížející nad proaktivními opatřeními členského státu o příslušnosti poskytovatele hostingových služeb.

Článek 5 stanoví požadavek, aby poskytovatelé hostingových služeb zavedli opatření za účelem neprodleného přístupu k obsahu uvedenému v hlášení od příslušného orgánu členského státu nebo orgánu Unie, ovšem aniž by stanovil požadavek odstranit takový ohlašovaný obsah či konkrétní termín provedení takového opatření. Stanoví také minimální náležitosti hlášení, postupy poskytovatelů hostingových služeb při předávání zpětné vazby vydávajícím orgánům a žádostech adresovaných orgánu, který obsah ohlásil, o bližší podrobnosti.

Článek 6 stanoví požadavek, aby poskytovatelé hostingových služeb případně uplatnili účinná a přiměřená proaktivní opatření. Stanoví postup, jak zajistit, aby určití poskytovatelé hostingových služeb (tj. ti, kteří obdrželi pravomocný příkaz k odstranění obsahu) případně uplatnili další proaktivní opatření s ohledem na riziko a míru expozice vůči teroristickému obsahu v rámci jejich služeb. Poskytovatel hostingových služeb musí ve věci nezbytných opatření spolupracovat s příslušným úřadem a, nelze-li dosáhnout dohody, orgán může opatření poskytovateli služeb uložit. Článek také stanoví postup přezkoumání rozhodnutí orgánu.

Článek 7 stanoví požadavek, aby poskytovatelé hostingových služeb uchovávali odstraněný obsah a související údaje pro účely přezkumného řízení a vyšetřování po dobu šesti měsíců. Tuto lhůtu lze prodloužil, aby bylo možné přezkumné řízení dokončit. Článek také stanoví požadavek, aby poskytovatelé hostingových služeb zavedli ochranná opatření s cílem znemožnit přístup k uchovávanému obsahu a souvisejícím údajům nebo jejich zpracování pro jiné účely.

Článek 8 ukládá poskytovatelům hostingových služeb povinnost vysvětlit jejich opatření proti teroristickému obsahu a zveřejňovat jednou za rok zprávy o transparentnosti týkající se opatření přijatých za tímto účelem.

Článek 9 stanoví konkrétní ochranná opatření týkající se využívání a provádění proaktivních opatření při používání automatizovaných nástrojů, aby bylo zajištěno, že jsou rozhodnutí přesná a řádně podložená.

Článek 10 od poskytovatelů hostingových služeb vyžaduje, aby ve vztahu k odstraňování obsahu, hlášení a proaktivním opatřením zavedli mechanismy pro podávání stížností a neprodlené šetření každé stížnosti.

Článek 11 ukládá poskytovatelům hostingových služeb povinnost zpřístupnit informace o odstranění poskytovateli obsahu, nebude-li příslušný orgán pro účely veřejné bezpečnosti vyžadovat, aby tyto informace nebyly sděleny.

Článek 12 vyžaduje, aby členské státy zajistily, že příslušné orgány budou mít k dispozici dostatečné kapacity a prostředky k plnění povinností vyplývajících z tohoto nařízení.

Článek 13 vyžaduje, aby členské státy spolupracovaly vzájemně a případně s Europolem, aby se zabránilo duplicitě a zásahům do šetření. Článek také dává členským státům a poskytovatelům hostingových služeb možnost využívat ke zpracování příkazů k odstranění obsahu a pro účely zpětné vazby a hlášení speciální nástroje, a to včetně nástrojů Europolu, a spolupracovat na proaktivních opatřeních. Od členských států také vyžaduje, aby měly zavedeny náležité komunikační kanály, které by při provádění a prosazování ustanovení tohoto nařízení zajišťovaly včasné předávání informací. Tento článek také poskytovatelům

hostingových služeb ukládá povinnost informovat příslušné orgány v případě, že se dozví o důkazech o teroristických trestných činech ve smyslu článku 3 směrnice (EU) 2017/541 o boji proti terorismu.

Článek 14 stanoví zřízení kontaktních míst ze strany poskytovatelů hostingových služeb i členských států, která by umožnila vzájemnou komunikaci, a to zejména v souvislosti s hlášením a příkazy k odstranění obsahu.

Článek 15 určuje příslušnosti členských států pro účely dohledu nad proaktivními opatřeními, stanovení sankcí a monitorování činností.

Článek 16 od poskytovatelů hostingových služeb, kteří nemají provozovnu v některém ze členských států, ale nabízejí služby v Unii, vyžaduje, aby v Unii jmenovali zákonného zástupce.

Článek 17 od členských států vyžaduje, aby určily orgány, které budou vydávat příkazy k odstranění obsahu, ohlašovat teroristický obsah, dohlížet na provádění proaktivních opatření a prosazovat výkon povinností podle tohoto nařízení.

Článek 18 stanoví, že členské státy mají povinnost stanovit pravidla pro sankce za neplnění požadavků, a uvádí kritéria, která mají členské státy zohlednit při stanovení druhu a výše sankcí. S ohledem na zvláštní význam neprodleného odstranění teroristického obsahu uvedeného v příkazu k odstranění je nutné zavést konkrétní pravidla pro finanční sankce za systematické porušování tohoto požadavku.

Článek 19 stanoví rychlejší a flexibilnější postupy změn šablon navržených pro účely příkazů k odstranění obsahu a ověřených kanálů pro hlášení prostřednictvím aktů v přenesené pravomoci.

Článek 20 stanoví podmínky, za kterých má Komise pravomoc přijmout akty v přenesené pravomoci, aby stanovila nezbytné změny šablon a technických požadavků na příkazy k odstranění obsahu.

Článek 21 po členských státech požaduje, aby shromažďovaly a hlásily konkrétní informace týkající se uplatňování nařízení s cílem pomoci Komisi při plnění jejích povinností podle článku 23. Komise zavede podrobný program pro monitorování výstupů, výsledků a dopadů tohoto nařízení.

Článek 22 stanoví požadavek, aby Komise podala zprávu o provádění tohoto nařízení dva roky poté, co vstoupí v platnost.

Článek 23 stanoví požadavek, aby Komise podala zprávu o hodnocení tohoto nařízení až tři roky poté, co vstoupí v platnost.

Článek 24 stanoví, že navrhované nařízení vstupuje v platnost dvacátým dnem po vyhlášení v Úředním věstníku Evropské unie a účinnosti nabude 6 měsíců po datu, kdy vstoupilo v platnost. Tato lhůta je navržena s ohledem na nezbytnost prováděcích opatření a naléhavost plné účinnosti pravidel navrhovaného nařízení. Tato šestiměsíční lhůta byla stanovena na základě předpokladu, že příslušná jednání proběhnou rychle.

2018/0331 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o prevenci šíření teroristického obsahu online

Příspěvek Evropské komise k zasedání vedoucích představitelů v Salcburku ve dnech 19.–20. září 2018

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[6],

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

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

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

(3) Přítomnost teroristického obsahu online má závažné negativní dopady na uživatele, občany a celou společnost, ale také na poskytovatele internetových služeb, na jejichž platformách se takový obsah nachází, neboť se tím narušuje důvěra jejich uživatelů a dochází poškozování jejich obchodních modelů. Vzhledem k tomu, že poskytovatelé online služeb hrají ústřední úlohu a mají k dispozici technologické prostředky

[6] Úř. věst. C , , s. .

a kapacity související s poskytovanými službami, nesou zvláštní společenskou odpovědnost za ochranu svých služeb před zneužitím teroristy a za boj proti teroristickému obsahu šířenému prostřednictvím jejich služeb.

(4) Abychom mohli omezit dostupnost teroristického obsahu online a náležitě řešit tento rychle se rozvíjející problém, je třeba doplnit úsilí v boji proti teroristickému obsahu online zahájené na úrovni Unie v roce 2015 v rámci dobrovolné spolupráce mezi členskými státy a poskytovateli hostingových služeb o jasný legislativní rámec. Legislativní rámec se snaží navázat na dobrovolné úsilí, které bylo posíleno doporučením Komise (EU) 2018/334[7], a reaguje na výzvy Evropského parlamentu, aby byla zintenzivněna opatření pro boj proti nezákonnému a škodlivému obsahu, a Evropské rady, aby došlo ke zlepšení automatického odhalování a odstraňování obsahu, jenž podněcuje k teroristickým činům.

(5) Uplatňováním tohoto nařízení by nemělo být dotčeno uplatňování článku 14 směrnice 2000/31/ES[8]. Opatření přijatá poskytovateli hostingových služeb v souladu s tímto nařízením, a to včetně proaktivních opatření, nesmí sama o sobě vést k tomu, že se na poskytovatele služeb přestane vztahovat výjimka z odpovědnosti stanovená příslušným ustanovením. Tímto nařízením nejsou dotčeny pravomoci vnitrostátních orgánů a soudů stanovit v konkrétních případech, kdy nejsou splněny podmínky pro výjimku z odpovědnosti dle článku 14 směrnice 2000/31/ES, odpovědnost poskytovatelů hostingových služeb.

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

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

(8) Právo na účinnou právní ochranu je zakotveno v článku 19 Smlouvy o EU a článku 47 Listiny základních práv Evropské unie. Každá fyzická nebo právnická osoba má právo u příslušného vnitrostátního soudu na účinnou právní ochranu před opatřeními

---

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

[8] 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).

přijatými dle tohoto nařízení, která mají negativní dopady na práva takové osoby. Toto právo zahrnuje zejména možnost poskytovatelů hostingových služeb a poskytovatelů obsahu se účinně bránit proti příkazům k odstranění obsahu u soudu členského státu, ve kterém orgány příkaz k odstranění obsahu vydaly.

(9) Aby se vyjasnilo, jaká opatření mají poskytovatelé hostingových služeb a příslušné orgány přijmout za účelem prevence šíření teroristického obsahu online, musí toto nařízení stanovit definici teroristického obsahu pro preventivní účely, která bude čerpat z definice teroristických trestných činů uvedené ve směrnici Evropského parlamentu a Rady (EU) 2017/541[9]. S ohledem na nutnost řešit nejškodlivější teroristickou propagandu na internetu musí definice postihovat materiál a informace, které podněcují, podporují a obhajují páchání teroristických trestných činů nebo podílení se na nich, uvádějí pokyny k páchání takových trestných činů nebo propagují účast na činnostech teroristické skupiny. Takové informace zahrnují zejména text, obrázky, zvukové nahrávky a videa. Při posuzování, zda je obsah teroristický ve smyslu tohoto nařízení, musí příslušné orgány i poskytovatelé hostingových služeb zohlednit faktory jako např. povahu a znění příslušného výroku či projevu, kontext, ve kterém byl učiněn, a jeho potenciál přivodit škodlivé důsledky, které by měly vliv na bezpečnost osob. Skutečnost, že byl materiál vytvořen teroristickou organizací nebo osobou uvedenou na příslušných seznamech EU, lze jej takové organizaci přičítat nebo je šířen jejím jménem, je při posouzení důležitým faktorem. Obsah šířený pro vzdělávací, žurnalistické či výzkumné účely je třeba náležitě chránit. Navíc by mělo být za teroristický obsah považováno vyjadřování radikálních, polemických či kontroverzních názorů ve veřejné diskuzi o citlivých politických otázkách.

(10) Má-li se toto opatření vztahovat také na online hostingové služby, ve kterých je šířen teroristický obsah, mělo by toto nařízení upravovat služby informační společnosti, které uchovávají informace poskytované příjemcem služby na jeho žádost a které takové uchovávané informace zpřístupňují třetím stranám bez ohledu na to, zda je taková činnost pouze technické, automatické a pasivní povahy. Takoví poskytovatelé služeb informační společnosti například zahrnují platformy sociálních médií, služby audiovizuálního přenosu prostřednictvím internetu (tzv. video streaming), služby sdílení videa, obrazového a zvukového materiálu, služby sdílení souborů a jiné cloudové služby v rozsahu, ve kterém zpřístupňují informace třetím stranám a webům, kde mohou uživatelé vkládat komentáře nebo recenze. Nařízení by se mělo také vztahovat na poskytovatele hostingových služeb s provozovnou mimo Unii, kteří ovšem nabízejí služby v rámci Unie, protože velká část poskytovatelů hostingových služeb vystavených v rámci svých služeb teroristickému obsahu online sídlí ve třetích zemích. To by mělo zajistit, že všechny společnosti působící na jednotném digitálním trhu splňují stejné požadavky, a to bez ohledu na zemi, kde mají provozovnu. K určení, zda poskytovatel služeb nabízí služby v Unii, je nutné posoudit, zda poskytovatel služeb umožňuje právnickým nebo fyzickým osobám v jednom či více členských státech využívat jeho služby. Avšak pouhá dostupnost webové stránky, e-mailové adresy a jiných kontaktních údajů poskytovatele služeb v jednom nebo více členských státech, posuzovaných odděleně, by neměla být dostatečnou podmínkou pro použití tohoto nařízení.

[9] 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).

(11) Pro stanovení působnosti tohoto nařízení musí být relevantní podstatné spojení s Unií. Existence takového podstatného spojení s Unií se předpokládá tehdy, má-li poskytovatel služeb provozovnu v Unii, nebo, v případě absence provozovny, na základě existence významného počtu uživatelů v jednom nebo více členských státech nebo zacílení činností na jeden nebo více členských států. Zacílení činností na jeden nebo více členských států lze určit na základě všech relevantních okolností, včetně takových faktorů, jako je používání jazyka či měny obecně používaných v daném členském státě nebo možnost objednání zboží či služeb. Zacílení činností na některý členský stát by mohlo být též odvozeno od dostupnosti aplikace v obchodě s aplikacemi příslušného členského státu, od poskytování místních reklam nebo reklam v jazyce používaném v příslušném členském státě nebo od řešení vztahů se zákazníky, např. poskytováním zákaznického servisu v jazyce obecně používaném v příslušném členském státě. Podstatné spojení je třeba předpokládat i v případě, že poskytovatel služeb zaměřuje svoje činnosti na jeden nebo více členských států, jak stanoví čl. 17 odst. 1 písm. c) nařízení Evropského parlamentu a Rady č. 1215/2012[10]. Na druhou stranu poskytování služby s cílem pouhého souladu se zákazem diskriminace stanoveným v nařízení Evropského parlamentu a Rady[11] (EU) 2018/302 nelze jen na základě tohoto důvodu pokládat za zaměření nebo zacílení činností na dané území v Unii.

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

(13) Je nutné harmonizovat postup a povinnosti vyplývající ze zákonných příkazů, které po posouzení příslušnými orgány, vyžadují po poskytovatelích hostingových služeb odstranit teroristický obsah nebo zamezit přístupu k němu. Členské státy budou mít volnost, co se týče výběru příslušných orgánů, a tento úkol budou moci uložit správním, donucovacím či soudním orgánům. S ohledem na rychlost šíření teroristického obsahu napříč online službami ukládá toto ustanovení poskytovatelům hostingových služeb povinnost zajistit, aby byl teroristický obsah uvedený v příkazu k odstranění obsahu odstraněn nebo přístup k němu zamezen od jedné hodiny od přijetí příkazu k odstranění obsahu. Rozhodnutí, zda dotyčný obsah odstranit nebo k němu zamezit přístup uživatelům v Unii, je na poskytovateli hostingových služeb.

(14) Příslušný orgán by měl příkaz k odstranění obsahu předat přímo adresátovi a kontaktnímu místu elektronickými prostředky umožňujícími vyhotovení písemného záznamu za podmínek, jež poskytovateli služeb umožňují ověřit pravost, včetně přesnosti data a času odeslání a přijetí příkazu, např. zabezpečenou e-mailovou poštou

---

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

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

a prostřednictvím platforem nebo jiných zabezpečených kanálů, včetně těch, které dá k dispozici poskytovatel služeb, a to v souladu s pravidly pro ochranu osobních údajů. Tento požadavek lze uspokojit zejména využitím kvalifikovaných služeb elektronického doporučeného doručování, jak stanoví nařízení Evropského parlamentu a Rady (EU) č. 910/2014[12].

(15) Hlášení ze strany příslušných úřadů nebo Europolu představuje účinný a rychlý způsob, jak poskytovatele hostingových služeb informovat o konkrétním obsahu v jejich službě. Tento mechanismus upozorňování poskytovatelů hostingových služeb na informace, které mohou být považovány za teroristický obsah, který poskytovateli hostingových služeb umožňuje posoudit soulad s jeho vlastními podmínkami, by měl zůstat k dispozici vedle příkazů k odstranění obsahu. Důležité je, aby poskytovatelé hostingových služeb taková hlášení prioritně posoudili a poskytli rychlou zpětnou vazbu o přijatých opatřeních. Konečné rozhodnutí, zda odstranit obsah, protože není v souladu s jejich podmínkami, leží i nadále na poskytovateli hostingových služeb. Při provádění tohoto nařízení v souvislosti s hlášením zůstává mandát Europolu stanovený nařízením (EU) 2016/794[13] nedotčen.

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

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

---

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

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

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

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

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

(21) Povinnost uchovávat obsah pro účely řízení správního či soudního přezkumu je nutná a důvodná s cílem zajištění účinných opatření soudní nápravy pro poskytovatele obsahu, jejichž obsah byl odstraněn nebo k němu byl zamezen přístup, a také zajištění obnovení takového obsahu do stavu, v jakém byl před odstraněním, v závislosti na výsledku přezkoumání. Tato povinnost uchovávat obsah pro účely vyšetřování a trestního stíhání je důvodná a nutná s ohledem na hodnotu, kterou může tento materiál přinést ve prospěch narušení či prevence teroristické činnosti. V případech, kdy společnosti odstraní materiál nebo zamezí přístupu k němu, a to zejména

prostřednictvím vlastních proaktivních opatření, a neinformují o tom příslušné orgány, protože vyhodnotí, že nespadá do působnosti článku 13 odst. 4 tohoto nařízení, nemusí donucovací orgány o existenci takového obsahu vědět. Proto je uchovávání obsahu pro účely prevence, odhalování vyšetřování a trestního stíhání teroristických trestných činů také důvodné. Pro tyto účely je vyžadované uchovávání omezeno na údaje, které jsou pravděpodobně napojeny na teroristické trestné činy, a mohou tudíž přispívat k trestnímu stíhání teroristických trestných činů nebo prevenci závažných rizik vůči veřejné bezpečnosti.

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

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

(24) Transparentnost pravidel poskytovatelů hostingových služeb ve vztahu k teroristickému obsahu je nezbytná pro posílení jejich odpovědnosti vůči uživatelům a důvěry občanů v jednotný digitální trh. Poskytovatelé hostingových služeb by měli zveřejňovat jednou za rok zprávy o transparentnosti, které budou obsahovat smysluplné informace o opatřeních přijatých v souvislosti s odhalováním, identifikací a odstraňováním teroristického obsahu.

(25) Postupy řešení stížností představují nezbytné ochranné opatření proti chybnému odstranění obsahu chráněného právem svobody projevu a informací. Poskytovatelé hostingových služeb proto musí zřídit uživatelsky vstřícné mechanismy pro podání stížností a zajistit, aby byly stížnosti řešeny neprodleně a zcela transparentně ve vztahu k poskytovateli obsahu. Požadavkem, aby poskytovatelé hostingových služeb obnovili obsah, který byl chybně odstraněn, není dotčena možnost prosazování vlastních podmínek poskytovatelů hostingových služeb na základě jiných důvodů.

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

(27) Aby se zabránilo duplikaci a případným zásahům do šetření, příslušné orgány se musí při vydávání příkazů k odstranění obsahu či zasílání hlášení poskytovatelům hostingových služeb vzájemně informovat, koordinovat činnosti a spolupracovat a v příslušných případech tak činit také ve spolupráci s Europolem. Při provádění ustanovení tohoto nařízení může Europol poskytovat podporu v souladu s aktuálním mandátem a stávajícím právním rámcem.

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

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

(30) Za účelem zprostředkování rychlé komunikace mezi příslušnými orgány a s poskytovateli hostingových služeb a prevence duplicitních činností mohou členské státy využívat nástroje vyvinuté Europolem, jako např. stávající aplikaci pro správu hlášení obsahu na internetu (Internet Referral Management application, IRMa) nebo následně vyvinuté nástroje.

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

(32) Příslušné orgány v členských orgánech by měly mít možnost využívat takové informace k přijetí vyšetřovacích opatření dostupných v rámci právních předpisů členského státu nebo Unie, a to včetně evropského předávacího příkazu dle nařízení o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech[14].

(33) Poskytovatelé hostingových služeb i členské státy musí zřídit kontaktní místa, která umožní rychlé zpracování příkazů k odstranění obsahu a hlášení. Na rozdíl od zákonného zástupce slouží kontaktní místo k provozním účelům. Kontaktní místo poskytovatele hostingových služeb může spočívat ve vyhrazeném prostředku, který umožní elektronické podání příkazů k odstranění obsahu a hlášení, a technických a personálních prostředcích umožňujících jejich rychlé zpracování. Kontaktní místo

[14] COM(2018) 225 final.

poskytovatele hostingových služeb se nemusí nacházet v Unii a poskytovatel hostingových služeb má možnost určit stávající kontaktní místo, pokud je takové kontaktní místo schopno plnit funkce stanovené tímto nařízením. Aby mohl být teroristický obsah odstraněn nebo přístup k němu zamezen od jedné hodiny od přijetí příkazu k odstranění obsahu, musí poskytovatelé hostingových služeb zajistit, že kontaktní místo bude dostupné 24 hodin denně, 7 dní v týdnu. Informace o kontaktním místě by měly zahrnovat informace o jazyce, ve kterém se lze na kontaktní místo obracet. Za účelem umožnění komunikace mezi poskytovateli hostingových služeb a příslušnými orgány nabádáme poskytovatele hostingových služeb, aby umožnili komunikaci v jednom z úředních jazyků Unie, ve kterém jsou dostupné jejich obchodní podmínky.

(34) Protože neexistuje požadavek, aby poskytovatelé služeb zajistili fyzickou přítomnost na území Unie, je nutné jednoznačně určit, do příslušnosti kterého členského státu spadá poskytovatel hostingových služeb nabízející služby v Unii. Obecně platí, že poskytovatel hostingových služeb spadá do příslušnosti členského státu, ve kterém má hlavní provozovnu nebo kde určil právního zástupce. Nicméně pokud jiný členský stát vydá příkaz k odstranění obsahu, jeho orgány by měly být schopné prosadit takové příkazy pomocí donucovacích opatření nerepresivní povahy, např. platba pokuty. Co se týče poskytovatele hostingových služeb, který nemá v Unii žádnou provozovnu ani určeného zákonného zástupce, členský stát by měl být i přesto schopen stanovit sankcích, a to za předpokladu, že bude respektována zásada *ne bis in idem*.

(35) Poskytovatelé hostingových služeb, kteří nemají provozovnu v Unii, musí písemně určit zákonného zástupce, aby zajistili plnění povinností stanovených tímto nařízením a jejich prosazování.

(36) Zákonný zástupce musí být právně zmocněn, aby jednal jménem poskytovatele hostingových služeb.

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

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

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

(40) Aby bylo možné v nezbytných případech provádět rychlé změny obsahu šablon, které budou sloužit pro účely tohoto nařízení, měla by být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování Evropské unie, aby mohla změnit přílohy I, II a III tohoto nařízení. Aby bylo možné zohlednit vývoj technologií a souvisejícího právního rámce, Komise by rovněž měla být zmocněna k přijímání aktů v přenesené pravomoci, aby toto nařízení mohla doplnit o technické požadavky na elektronické prostředky využívané příslušnými orgány k přenosu příkazů k odstranění obsahu. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě o zdokonalení tvorby právních předpisů[15] ze dne 13. dubna 2016. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států, přičemž jejich odborníci mají automaticky přístup na setkání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

(41) Členské státy musí shromažďovat informace o zavádění právních předpisů. Za účelem získání informací pro hodnocení právního předpisu je nutné stanovit podrobný program monitorování výstupů, výsledků a dopadů tohoto nařízení.

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

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

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

PŘIJALY TOTO NAŘÍZENÍ:

ODDÍL I
OBECNÁ USTANOVENÍ

Článek 1
Předmět a oblast působnosti

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

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

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

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

Článek 2
Definice

Pro účely tohoto nařízení se rozumí:

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

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

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

   a) provozovnu poskytovatele hostingových služeb v Unii;

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

   c) zaměření činností na jeden nebo více členských státech.

4) „teroristickými trestnými činy“ trestné činy ve smyslu čl. 3 odst. 1 směrnice (EU) 2017/541;

5) „teroristickým obsahem“ jedna nebo více z těchto informací:

   a) podněcování k teroristickým trestným činům, nebo jejich obhajování, včetně jejich glorifikace představující riziko, že takové činy budou spáchány;

   b) podpora napomáhání teroristickým trestným činům;

c) napomáhá činnostem teroristické skupiny, zejména podporou účasti v teroristické skupině či podporou teroristické skupiny ve smyslu čl. 2 odst. 3 směrnice (EU) 2017/541;

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

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

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

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

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

ODDÍL II
Opatření pro prevenci šíření teroristického obsahu na internetu

Článek 3
Povinnosti náležité péče

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

2. Poskytovatelé hostingových služeb zahrnou do svých podmínek ustanovení zamezující šíření teroristického obsahu a tato ustanovení uplatňují.

Článek 4
Příkazy k odstranění

1. Příslušný orgán je oprávněn vydat rozhodnutí, kterým se od poskytovatele hostingových služeb požaduje, aby teroristický obsah odstranil nebo znemožnil k němu přístup.

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

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

a) identifikaci příslušného orgánu, který vydává příkaz k odstranění, a autentizaci příkazu k odstranění ze strany příslušného orgánu;

b) odůvodnění, proč je obsah považován za teroristický, přinejmenším prostřednictvím odkazu na kategorie teroristického obsahu uvedené v čl. 2 odst. 5;

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

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

e) razítko s datem a časem vydání;

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

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

4. Na žádost poskytovatele hostingových služeb nebo poskytovatele obsahu předloží příslušný orgán podrobné odůvodnění, aniž je dotčena povinnost poskytovatele hostingových služeb splnit příkaz k odstranění ve lhůtě stanovené v odstavci 2.

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

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

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

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

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

Článek 5
Hlášení

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

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

3. Hlášení je adresováno do hlavní provozovny poskytovatele hostingových služeb nebo zákonnému zástupci určenému poskytovatelem služeb podle článku 16

a předáno kontaktnímu místu uvedenému v čl. 14 odst. 1. Tato hlášení se zasílají elektronicky.

4. Hlášení obsahuje dostatečně podrobné informace, včetně důvodů, proč je obsah považován za teroristický, URL a v případě potřeby doplňujících informací umožňujících identifikaci uvedeného teroristického obsahu.

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

6. Poskytovatel hostingových služeb neprodleně informuje příslušný orgán nebo příslušný subjekt Unie o výsledku posouzení a o načasování opatření přijatých na základě hlášení.

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

Článek 6
Proaktivní opatření

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

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

   a) prevence opětovného nahrání obsahu, který byl již dříve odstraněn nebo k němuž byl odepřen přístup, protože je považován za teroristický;

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

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

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

3. Jestliže se příslušný orgán uvedený v čl. 17 odst. 1 písm. c) domnívá, že proaktivní opatření přijatá a nahlášená podle odstavce 2 nejsou dostatečná pro zmírnění a řízení rizika a úrovně expozice, může poskytovatele hostingových služeb požádat, aby přijal zvláštní dodatečná proaktivní opatření. Za tímto účelem spolupracuje poskytovatel hostingových služeb s příslušným orgánem uvedeným v čl. 17 odst. 1

písm. c) s cílem určit konkrétní opatření, která poskytovatel hostingových služeb zavede, a stanovit hlavní cíle a referenční hodnoty, jakož i lhůty pro jejich provedení.

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

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

Článek 7
Uchovávání obsahu a souvisejících údajů

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

   a) správního nebo soudního přezkumu;

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

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

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

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

ODDÍL III
ZÁRUKY A ODPOVĚDNOST

Článek 8
Povinnosti týkající se transparentnosti

1. Poskytovatelé hostingových služeb vymezí ve svých podmínkách svou politiku týkající se prevence šíření teroristického obsahu, včetně případného smysluplného

vysvětlení fungování aktivních opatření, včetně používání automatizovaných nástrojů.

2. Poskytovatelé hostingových služeb zveřejňují výroční zprávy o transparentnosti, pokud jde o opatření přijatá proti šíření teroristického obsahu.

3. Zprávy o transparentnosti musejí obsahovat alespoň tyto údaje:

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

   b) informace o opatřeních poskytovatele hostingových služeb v zájmu prevence opětovného nahrání obsahu, který byl již dříve odstraněn nebo k němuž byl znemožněn přístup, protože je považován za teroristický;

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

   d) přehled a výsledky řízení o stížnostech.

Článek 9

Záruky týkající se používání a zavádění proaktivních opatření

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

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

Článek 10

Mechanismy pro podávání a vyřizování stížností

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

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

Článek 11

Informace pro poskytovatele obsahu

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

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

3. Povinnost podle odstavců 1 a 2 se nevztahuje na případy, kdy příslušný orgán rozhodne, že by z důvodu veřejné bezpečnosti, jako je prevence, vyšetřování, odhalování a stíhání teroristických trestných činů, neměly být zveřejněny žádné informace, a to po dobu nezbytně nutnou, avšak ne delší než [4] týdny od uvedeného rozhodnutí. V takovém případě poskytovatel hostingových služeb nezveřejní žádné informace o odstranění teroristického obsahu nebo znemožnění přístupu k němu.

ODDÍL IV
Spolupráce mezi příslušnými orgány, subjekty Unie a poskytovateli hostingových služeb

Článek 12
Kapacity příslušných orgánů

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

Článek 13
Spolupráce mezi poskytovateli hostingových služeb, příslušnými orgány a případně příslušnými subjekty Unie

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

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

3. Členské státy a poskytovatelé hostingových služeb se mohou rozhodnout, že využijí specializované nástroje, případně včetně nástrojů zavedených příslušnými subjekty Unie, jako je Europol, a to zejména za účelem usnadnění:

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

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

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

4. Pokud se poskytovatelé hostingových služeb dozví o jakémkoli důkazu teroristických trestných činů, neprodleně uvědomí orgány odpovědné za vyšetřování a stíhání trestných činů v dotyčném členském státě nebo kontaktní místo v členském státě podle čl. 14 odst. 2, kde mají svou hlavní provozovnu nebo zákonného zástupce. V případě pochybností mohou poskytovatelé hostingových služeb předat tyto informace Europolu za účelem provedení příslušných následných opatření.

Článek 14
Kontaktní místa

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

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

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

ODDÍL V
PROVÁDĚNÍ A VÝKON

Článek 15
Příslušnost

1. Členský stát, v němž se nachází hlavní provozovna poskytovatele hostingových služeb, je příslušný pro účely článků 6, 18 a 21. Poskytovatel hostingových služeb, jehož hlavní provozovna není v některém z členských států, se považuje za poskytovatele hostingových služeb, který spadá do příslušnosti členského státu, v němž má bydliště nebo je usazen zákonný zástupce uvedený v článku 16.

2. Pokud poskytovatel hostingových služeb nejmenuje zákonného zástupce, jsou příslušné všechny členské státy.

3. Pokud příkaz k odstranění podle čl. 4 odst. 1 vydal orgán jiného členského státu, má tento členský stát příslušnost přijmout donucovací opatření v souladu se svým vnitrostátním právem za účelem výkonu příkazu k odstranění.

Článek 16
Zákonný zástupce

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

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

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

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

ODDÍL VI
ZÁVĚREČNÁ USTANOVENÍ

Článek 17
Určení příslušných orgánů

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

   a) vydávání příkazů k odstranění podle článku 4.

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

   c) dohledu na provádění proaktivních opatření podle článku 6;

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

2. Nejpozději do [*šest měsíců od vstupu tohoto nařízení v platnost*] oznámí členský stát příslušné orgány uvedené v odstavci 1 Komisi. Komise toto hlášení a veškeré jeho změny zveřejní v *Úředním věstníku Evropské unie*.

Článek 18
Sankce

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

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

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

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

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

   e) článku 7 (uchovávání údajů);

   f) článku 8 (transparentnost);

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

   h) článku 10 (postupy pro podávání stížností);

   i) článku 11 (informace pro poskytovatele obsahu)

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

   k) čl. 14 odst. 1 (kontaktní místa);

l) článku 16 (určení zákonného zástupce).

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

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

a) povahy, závažnosti a doby trvání porušení;

b) záměrné či nedbalostní povahy porušení;

c) předchozích porušení předpisů odpovědnou právnickou osobou;

d) finanční síly odpovědné právnické osoby;

e) úrovně spolupráce poskytovatele hostingových služeb s příslušnými orgány.

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

Článek 19
Technické požadavky a změny šablon příkazů k odstranění

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

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

Článek 20
Výkon přenesené pravomoci

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

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

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

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

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

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

Článek 21
Monitorování

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

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

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

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

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

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

Článek 22
Zpráva o provádění

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

Článek 23
Hodnocení

Nejdříve [*tři roky ode dne použitelnosti tohoto nařízení*] provede Komise hodnocení tohoto nařízení a předloží Evropskému parlamentu a Radě zprávu o jeho uplatňování, včetně fungování účinnosti ochranných mechanismů. V případě potřeby ke zprávě připojí legislativní

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

Článek 24
Vstup v platnost

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

Použije se ode dne [šest měsíců po vstupu v platnost].

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

V Bruselu dne

Za Evropský parlament	*Za Radu*
předseda	*předseda*