EVROPSKÁ
KOMISE

V Bruselu dne 14.2.2024
COM(2024) 64 final

ZPRÁVA KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

o provádění nařízení (EU) 2021/784 o potírání šíření teroristického obsahu online

{SWD(2024) 36 final}

1. SHRNUTÍ

Nařízení (EU) 2021/784 o potírání šíření teroristického obsahu online poskytuje členským státům právní rámec na evropské úrovni, jehož cílem je chránit občany před vystavením teroristickému materiálu online. Nařízení se snaží zajistit řádné fungování jednotného digitálního trhu tím, že se zaměřuje na boj proti zneužívání hostingových služeb k veřejnému šíření teroristického obsahu online. Jeho cílem je zabránit tomu, aby teroristé využívali internet k šíření svých myšlenek za účelem zastrašování, radikalizace, náboru a usnadnění teroristických útoků. To je obzvláště důležité v nynějším kontextu konfliktů a nestability, který má dopad na bezpečnost Evropy. Ruská útočná válka proti Ukrajině a teroristický útok, který 7. října 2023 spáchal Hamás proti Izraeli, měly za následek nárůst teroristického obsahu šířeného online.

Regulační rámec pro řešení nelegálního obsahu online byl dále posílen vstupem nařízení o digitálních službách v platnost dne 16. listopadu 2022. Nařízení o digitálních službách upravuje povinnosti v oblasti digitálních služeb, jde-li o zprostředkovatele, jejichž úloha spočívá ve spojování spotřebitelů s obsahem, službami a zbožím, a tak lépe chrání uživatele online a přispívá k bezpečnějšímu online prostředí.

Nařízení o potírání šíření teroristického obsahu online je použitelné ode dne 7. června 2022. Podle článku 22 nařízení předloží Komise Evropskému parlamentu a Radě zprávu o uplatňování nařízení („zpráva o provádění“).

Tato zpráva o provádění vychází z posouzení informací poskytnutých členskými státy, Europolem a poskytovateli hostingových služeb v souladu s povinnostmi stanovenými v nařízení. Na základě tohoto posouzení lze hlavní zjištění týkající se provádění nařízení shrnout takto:

- Ke dni 31. prosince 2023 **23 členských států** určilo příslušný orgán (příslušné orgány) s pravomocí vydávat příkazy k odstranění, jak je stanoveno v nařízení[1]. Seznam orgánů členských států je k dispozici na internetových stránkách Komise a je pravidelně aktualizován[2].

- Ke dni 31. prosince 2023 obdržela Komise informace o nejméně **349 příkazech k odstranění teroristického obsahu** vydaných příslušnými orgány šesti členských států (Španělska, Rumunska, Francie, Německa, Česka a Rakouska), které ve většině případů vedly k rychlým následným opatřením ze strany poskytovatelů hostingových služeb k odstranění teroristického obsahu nebo zablokování přístupu k němu. To dokazuje, že nástroje stanovené nařízením se začínají používat a úspěšně díky nim dochází k rychlému odstranění teroristického obsahu ze strany poskytovatelů hostingových služeb podle čl. 3 odst. 3. Podle informací, které Komise obdržela, nebyly tyto příkazy k odstranění napadeny.

[1] V online rejstříku, který Komise zřídila podle čl. 12 odst. 4 nařízení, jsou uvedeny příslušné orgány uvedené v čl. 12 odst. 1 a kontaktní místo určené nebo zřízené podle čl. 12 odst. 2 pro každý příslušný orgán. Rejstřík je pravidelně aktualizován na základě oznámení členských států. Seznam vnitrostátních příslušných orgánů a kontaktních míst (europa.eu).

[2] Seznam vnitrostátních příslušných orgánů a kontaktních míst.

- Při uplatňování nařízení, obzvláště při zpracovávání příkazů k odstranění, probíhá mezi příslušnými orgány členských států a Europolem, zejména jednotkou EU pro oznamování internetového obsahu, **dobrá koordinace**.
- Dne 3. července 2023 byl spuštěn nástroj Europolu „**PERCI**“[3]. Tento nástroj úspěšně používaly některé členské státy k předávání příkazů k odstranění i k hlášení[4]. Španělské, německé, rakouské, francouzské a české příslušné orgány tento nástroj použily k předání příkazů k odstranění. Celkově bylo v nástroji PERCI od jeho spuštění 3. července do 31. prosince 2023 zpracováno nejméně 14 615 hlášení.
- Ačkoli nařízení neobsahuje žádná zvláštní opatření týkající se hlášení, podle informací, které Komise obdržela, došlo od vstupu nařízení v platnost také ke **zvýšení schopnosti reakce na hlášení** ze strany poskytovatelů hostingových služeb.
- Na základě informací, které má Komise k dispozici, nebyl ke dni 31. prosince 2023 žádný poskytovatel hostingových služeb považován za vystaveného teroristickému obsahu ve smyslu čl. 5 odst. 4 nařízení. Takové zjištění by bylo předpokladem pro uplatnění zvláštních opatření stanovených v uvedeném článku. Poskytovatelé hostingových služeb nicméně podle zpráv o transparentnosti, které poskytli, přijali opatření **proti zneužívání svých služeb** k šíření teroristického obsahu, zejména přijetím zvláštních podmínek a uplatněním dalších ustanovení a opatření k omezení šíření teroristického obsahu.
- Poskytovatelé hostingových služeb rovněž přijali opatření k oznamování **bezprostředního ohrožení života** podle čl. 14 odst. 5 nařízení.

Co se týče **menších poskytovatelů hostingových služeb**, Komise v roce 2021 zveřejnila výzvu k podávání návrhů za účelem jejich podpory při provádění nařízení. Komise v roce 2022 vybrala tři projekty (viz oddíl 4.8), které zahájily svou činnost v roce 2023 a již přinesly určité výsledky při poskytování podpory malým podnikům v zájmu dosažení souladu s nařízením.

Zasláním **výzvy** dne 26. ledna 2023 zahájila Komise řízení o nesplnění povinnosti proti 22 členským státům, které neurčily příslušné orgány dle čl. 12 odst. 1 nařízení a nesplnily povinnosti dle čl. 12 odst. 2 a 3 a čl. 18 odst. 1 nařízení[5]. Po zahájení těchto řízení o nesplnění povinnosti se zvýšil počet členských států, které oznámily příslušné orgány odpovědné za zpracovávání příkazů k odstranění, což se odráží v informacích zveřejněných v online rejstříku[6]. Kromě toho bylo do 21. prosince 2023 uzavřeno 11 případů nesplnění povinnosti zahájených v lednu 2023[7].

[3] Nástroj PERCI *(Plateforme Européenne de Retraits des Contenus illégaux sur Internet)* je platforma pro odstraňování nelegálního obsahu online, kterou vyvinul a spravuje Europol. Podporuje provádění nařízení tím, že kromě jiných funkcí poskytuje poskytovatelům hostingových služeb technické řešení pro zpracování hlášení a příkazů k odstranění.

[4] Hlášení tvoří mechanismus upozorňování poskytovatelů hostingových služeb umožňující poskytovateli hostingových služeb, aby sám dobrovolně posoudil soulad tohoto obsahu se svými vlastními podmínkami. V nařízení (40. bod odůvodnění) se uvádí, že hlášení prokázala svou účinnost a měla by zůstat k dispozici vedle příkazů k odstranění.

[5] Viz tisková zpráva: Teroristický obsah online (europa.eu).

[6] Seznam vnitrostátních příslušných orgánů a kontaktních míst (europa.eu). V online rejstříku jsou informace o orgánech 23 členských států příslušných k vydávání příkazů k odstranění podle čl. 12 odst. 1 písm. a).

[7] Finsko, Malta, Česko, Dánsko, Rumunsko, Švédsko, Lotyšsko, Španělsko, Litva, Rakousko a Slovensko.

Na základě informací obdržených od členských států a Europolu a poskytnutých poskytovateli hostingových služeb Komise vyhodnotila, že uplatňování nařízení mělo **pozitivní dopad** na omezení šíření teroristického obsahu online.

2. SOUVISLOSTI

Nařízení vstoupilo v platnost dne 7. června 2022. Jeho cílem je zajistit řádné fungování jednotného digitálního trhu tím, že se zaměřuje na boj proti zneužívání hostingových služeb k veřejnému šíření teroristického obsahu online. Poskytuje členským státům cílené nástroje k boji proti šíření teroristického obsahu online v podobě příkazů k odstranění a umožňuje členským státům požadovat po poskytovatelích hostingových služeb všech velikostí, aby přijali konkrétní opatření na ochranu svých služeb před zneužitím teroristickými subjekty, jsou-li vystaveny teroristickému obsahu.

Od vstupu nařízení o digitálních službách v platnost dne 16. listopadu 2022 je navíc regulační prostředí rozšířeno o horizontální právní předpisy s širokou působností, jejichž cílem je zajištění bezpečnějšího digitálního prostoru pro spotřebitele, účinná opatření proti nelegálnímu obsahu a transparentnější podmínky poskytování služeb. Nařízení o digitálních službách dává Komisi dostatečné dohledové, vyšetřovací a donucovací pravomoci k přijímání opatření vůči velmi velkým online platformám a vyhledávačům. Jde mimo jiné o žádosti o informace, vyšetřování činností společností v oblasti moderování obsahu a možnost ukládání pokut.

Na základě nařízení o digitálních službách je možné zabývat se všemi formami nelegálního obsahu, přičemž Komise je oprávněna vyzývat platformy k poskytnutí údajů prokazujících, že platformy plní své vlastní závazky týkající se odstraňování obsahu. Nařízení o teroristickém obsahu online však poskytuje ještě silnější nástroj pro tuto specifickou formu nelegálního obsahu, a to díky právní povinnosti odstranit obsah do jedné hodiny od obdržení příkazu k odstranění a účinným sankčním mechanismům.

Jak upozorňuje Europol ve zprávách o stavu a vývoji terorismu[8] zveřejněných v posledních letech, teroristé hojně využívají internet k šíření svých myšlenek, aby zastrašovali, radikalizovali, verbovali a usnadňovali teroristické útoky. Dobrovolná opatření a nezávazná doporučení sice přinesla výsledky, pokud jde o snížení dostupnosti teroristického obsahu online, ale omezení, včetně malého počtu poskytovatelů hostingových služeb, kteří přijali dobrovolné mechanismy[9], jakož i roztříštěnost procesních pravidel v členských státech omezily účinnost a efektivitu spolupráce mezi členskými státy a poskytovateli hostingových služeb a způsobily, že bylo nutné zavést regulační opatření[10]. Pro potírání šíření teroristického obsahu online má tedy klíčový význam účinné uplatňování nařízení. Komise v tomto procesu aktivně podporuje vnitrostátní příslušné orgány.

[8] Zprávy Europolu o stavu a vývoji terorismu z roku 2023 https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2023.pdf a 2022 https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

[9] Evropská komise, (2018) Posouzení dopadů připojené k návrhu nařízení o prevenci šíření teroristického obsahu online, SWD(2018) 408 final, navštíveno dne 4.5.2023 na adrese: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN

[10] Tamtéž.

Podle článku 22 nařízení měla Komise povinnost předložit Evropskému parlamentu a Radě do 7. června 2023 zprávu o uplatňování nařízení („zprávu o provádění“) vycházející z informací poskytnutých členskými státy, jež se zase částečně opíraly o informace poskytnuté poskytovateli hostingových služeb (článek 21). Prodlení při předložení zprávy o provádění je způsobeno pozdním předáním klíčových informací od členských států a poskytovatelů hostingových služeb Komisi. Bylo však považováno za důležité zohlednit ve zprávě o provádění také používání nástroje PERCI, který byl uveden do provozu 3. července 2023 a od té doby se používá ke zpracování příkazů k odstranění podle nařízení.

Cílem této zprávy o provádění je pouze poskytnout věcný přehled o příslušných záležitostech týkajících se uplatňování nařízení. Neobsahuje žádné výklady nařízení a nevyjadřuje žádné stanovisko k výkladům nebo jiným opatřením přijatým při uplatňování nařízení.

V souladu s čl. 21 odst. 2 nařízení měla Komise do stejného data (7. června 2023) zavést podrobný program monitorování výstupů, výsledků a dopadů nařízení. Konkrétněji by měl program monitorování stanovit ukazatele, prostředky a intervaly shromažďování údajů a dalších potřebných důkazů. Tento program je vymezen v doprovodném pracovním dokumentu útvarů. Stanoví opatření, která mají Komise a členské státy přijmout při shromažďování a analýze údajů a dalších důkazů za účelem monitorování pokroku a dopadů nařízení a provádění hodnocení nařízení podle jeho článku 23.

3. CÍL A METODIKA ZPRÁVY

Cílem této zprávy je posoudit uplatňování nařízení a jeho dosavadní dopad na omezení šíření teroristického obsahu online. To zahrnuje opatření přijatá členskými státy a poskytovateli hostingových služeb, jako jsou změny jejich podmínek poskytování služeb a pokynů pro komunitu, a jejich plnění příkazů k odstranění a schopnost reakce na ně.

Za tímto účelem Komise shromáždila informace od členských států, jednotky Europolu pro oznamování internetového obsahu (jednotky EU pro oznamování internetového obsahu) a poskytovatelů hostingových služeb, včetně informací obsažených ve zprávách o transparentnosti a monitorování podle článků 7, 8 a 21 nařízení. Informace podle článků 8 a 21 byly obdrženy od 18 členských států. Informace o opatřeních přijatých poskytovateli hostingových služeb byly shromážděny prostřednictvím jejich výročních zpráv o transparentnosti, Europolu a přímé dobrovolné komunikace s útvary Komise. Tato zpráva o provádění zahrnuje informace, které Komise obdržela do 31. prosince 2023.

Povinnosti v oblasti monitorování a transparentnosti (články 21, 7 a 8)

Pro účely vypracování zprávy o provádění jsou členské státy podle čl. 21 odst. 1 nařízení povinny shromažďovat informace od svých příslušných orgánů a poskytovatelů hostingových služeb, kteří spadají do jejich jurisdikce, a tyto informace každoročně do 31. března zasílat Komisi. Jde mimo jiné o informace o opatřeních, která tyto orgány přijaly v souladu s nařízením v předchozím kalendářním roce. Ustanovení čl. 21 odst. 1 uvádí druh informací, které by členské státy měly shromažďovat o opatřeních přijatých k dosažení souladu s nařízením, jako jsou podrobnosti o

příkazech k odstranění, počtu žádostí o přístup k obsahu zachovávanému za účelem umožnění vyšetřování, postupech pro podávání stížností a o správních nebo soudních přezkumných řízeních.

Podle čl. 7 odst. 1 nařízení poskytovatelé hostingových služeb ve svých podmínkách jasně vymezí svou politiku zaměřenou na potírání šíření teroristického obsahu, přičemž v příslušných případech mimo jiné věcně vysvětlí fungování zvláštních opatření.

Kromě toho podle čl. 7 odst. 2 nařízení poskytovatel hostingových služeb, který v daném kalendářním roce přijal opatření proti šíření teroristického obsahu, nebo se od něj požadovalo, aby přijal opatření podle nařízení, zveřejní za daný rok zprávu o transparentnosti týkající se těchto opatření. Tato zpráva by měla být zveřejněna do 1. března následujícího roku.

Ustanovení čl. 7 odst. 3 nařízení stanoví minimální informace, které by tyto zprávy o transparentnosti měly obsahovat, jako jsou opatření přijatá k identifikaci teroristického obsahu a znemožnění přístupu k němu, počet odstraněných a/nebo obnovených položek a výsledky stížností.

Podle článku 8 nařízení zveřejňují určené příslušné orgány členských států výroční zprávy o transparentnosti týkající se jejich činností podle nařízení. V čl. 8 odst. 1 se uvádějí minimální informace, které by tyto zprávy měly obsahovat[11].

Ke dni 31. prosince 2023 osmnáct členských států zaslalo Komisi informace o svých opatřeních přijatých v souladu s nařízením a 23 členských států určilo orgán(y) s pravomocí vydávat příkazy k odstranění, jak je stanoveno v nařízení.

4. KONKRÉTNÍ POSUZOVANÉ BODY

4.1 PŘÍKAZY K ODSTRANĚNÍ (článek 3)

Ke dni 31. prosince 2023 byla Komise informována celkem o nejméně 349 příkazech k odstranění, které španělské, rumunské, francouzské, německé, rakouské a české příslušné orgány zaslaly sítím Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L., FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net a Catbox.

62 příkazů k odstranění zaslal příslušný orgán Španělska CITCO (*Centro de Inteligencia contra el Terrorismo y el Crimen Organizado*), dva příkazy k odstranění zaslal příslušný orgán Rumunska ANCOM (*Autoritatea Națională pentru Administrare și Reglementare în Comunicații*) a 26 příkazů k odstranění zaslal příslušný orgán Francie OCLCTIC (*L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication*). Od teroristického útoku Hamásu proti Izraeli zaslal německý příslušný orgán (*BKA – Bundeskriminalamt*) 249 příkazů k odstranění.

[11] Viz znění nařízení (EU) 2021/784, čl. 8 odst. 1 https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32021R0784

Španělský příslušný orgán předal 62 příkazů k odstranění: 18 před spuštěním nástroje PERCI a 44 jeho prostřednictvím. Poskytl podrobný popis předávání prvních vydaných příkazů k odstranění a následných opatření, což je velmi důležité pro lepší pochopení důsledků a účinků nařízení.

První dva příkazy k odstranění vydal příslušný orgán Španělska dne 24. dubna 2023[12]. Souvisely se dvěma položkami teroristického obsahu, z nichž jedna se týkala pravicového terorismu a druhá džihádismu. Obsah, který byl předmětem prvního příkazu k odstranění, byl dokument ve formátu PDF zveřejněný na síti Telegram s neomezeným přístupem, který obhajoval teroristické násilí a oslavoval pravicové teroristické útoky. Druhá položka teroristického obsahu, která byla předmětem příkazu k odstranění, se týkala videa se záběry džihádistů z teroristické organizace Islámský stát v boji, které bylo nahráno na stránky Internet Archive. Tyto dvě položky byly z obou platforem odstraněny do jedné hodiny, tedy v souladu s čl. 3 odst. 3 nařízení. V posouzení poskytnutém španělským příslušným orgánem bylo vysvětleno, že se rozhodl pro příkaz k odstranění namísto hlášení ze dvou hlavních důvodů: splnění požadavků nařízení týkajících se příkazů k odstranění a naléhavosti. Poté zaslal španělský příslušný orgán další příkazy k odstranění.

Španělský orgán upozornil na problémy spojené s používáním webového formuláře jedním poskytovatelem hostingových služeb (Meta) pro přijímání příkazů k odstranění namísto zajištění přímého kontaktního místa. Tento webový formulář také vedl k problémům při komunikaci s příslušným orgánem členského státu, v němž se nachází hlavní provozovna poskytovatele hostingových služeb.

Francouzský příslušný orgán vydal první příkaz k odstranění 13. července 2023 platformě pro sdílení (Justpaste.it), která teroristický obsah odstranila do jedné hodiny. Cíleným obsahem byla propaganda ze strany al-Káidy, konkrétně ze strany mediálního orgánu Rikan Ka Mimber, který patří do její indické odnože, organizace al-Káida na Indickém subkontinentu. Úplné odstranění obsahu bylo potvrzeno v platformě Europolu PERCI.

Německý příslušný orgán vydal dne 16. října šest, 18. října šestnáct a 24. října 2023 pět příkazů k odstranění zaměřených na propagandu Hamásu a Palestinského islámského džihádu. Přístup k obsahu byl v EU zablokován v souladu s čl. 3 odst. 3 nařízení. Německý příslušný orgán nejprve zaslal hlášení a následně vydal příkazy k odstranění, protože na tato hlášení nebylo reagováno. Po útoku hnutí Hamás dne 7. října 2023 zaslal německý příslušný orgán 249 příkazů k odstranění, a to převážně síti Telegram.[13]

Český příslušný orgán vydal dva příkazy k odstranění síti X, rakouský příslušný orgán vydal osm příkazů k odstranění síti Telegram.

Pokud jde o používání webového formuláře k přijímání příkazů k odstranění jedním poskytovatelem hostingových služeb, španělské orgány uvedly dva problémy: 1) v souvislosti s čl. 3 odst. 2 nařízení webový formulář neumožňuje příslušným orgánům členských států zasílat informace o platných postupech a lhůtách před vydáním prvního příkazu k odstranění poskytovateli hostingových služeb; 2) v souvislosti s čl. 4 odst. 1 webový formulář neumožňuje

[12] Ministerio del Interior | El CITCO culmina la retirada de Internet de dos contenidos que alentaban al terrorismo
[13] Podle informací, které má Komise k dispozici.

předat kopii příkazu k odstranění současně příslušnému orgánu členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu, a právnímu zástupci poskytovatele hostingových služeb.

4.2 PŘESHRANIČNÍ PŘÍKAZY K ODSTRANĚNÍ (článek 4)

V případě prvních dvou příkazů k odstranění vydaných v dubnu 2023 nemohl španělský příslušný orgán zaslat kopie orgánu členského státu, v němž měl poskytovatel hostingových služeb svou hlavní provozovnu nebo svého právního zástupce, jelikož žádný z těchto dvou poskytovatelů hostingových služeb neměl v té době hlavní provozovnu v EU, ani neurčil právního zástupce v EU. V případě následných příkazů k odstranění zaslal španělský příslušný orgán kopie příslušnému orgánu členského státu, v němž měl poskytovatel hostingových služeb svou hlavní provozovnu nebo v němž určil svého právního zástupce.

Členské státy uvádějí, že předávání příkazů k odstranění poskytovatelům hostingových služeb se sídlem ve třetích zemích, kteří dosud nesplnili svou povinnost jmenovat právního zástupce v EU, představuje problém. V této souvislosti Komise podpořila členské státy s cílem zajistit, aby poskytovatelé hostingových služeb splnili svou povinnost jmenovat právního zástupce v EU a poskytnout kontaktní místo (čl. 15 odst. 1 nařízení), např. e-mailovou adresu, pro zajištění okamžité reakce. Komise dále na různých fórech, včetně internetového fóra EU, připomněla poskytovatelům hostingových služeb jejich povinnosti.

Podle informací, které má Komise k dispozici, dosud žádný příslušný orgán členského státu, v němž má poskytovatel hostingových služeb hlavní provozovnu, nepřezkoumal příkaz k odstranění podle článku 4 nařízení, aby určil, zda závažně nebo zjevně neporušuje nařízení nebo základní práva a svobody, neboť dosud nebyla podána žádná odůvodněná žádost o přezkum. V důsledku toho dosud žádný orgán neshledal, že by příkaz k odstranění takovým způsobem porušoval toto nařízení nebo základní práva.

Žádný poskytovatel hostingových služeb dosud neobnovil obsah (nebo přístup k němu), který byl předmětem příkazu k odstranění, na základě přezkumu v souladu s článkem 4 nařízení, protože tento přezkum a žádosti o obnovení dosud nebyly uskutečněny. Nejsou tedy k dispozici žádné informace o tom, jak dlouho obvykle trvá obnovení obsahu nebo přístupu k němu, ani o „nezbytných krocích“, které poskytovatelé hostingových služeb přijali k obnovení obsahu nebo přístupu k němu.

4.3 PROSTŘEDKY NÁPRAVY (článek 9)

Podle informací, které má Komise k dispozici, poskytovatelé hostingových služeb dosud nenapadli příkazy k odstranění nebo rozhodnutí podle čl. 5 odst. 4 u příslušných soudů. Jeden poskytovatel hostingových služeb nicméně tvrdil, že provedení příkazu k odstranění není možné.

Podle informací poskytnutých členskými státy[14] má nejméně dvanáct členských států zavedeny „účinné postupy“, které poskytovatelům hostingových služeb a poskytovatelům obsahu umožňují napadnout příkaz k odstranění vydaný příslušným orgánem a/nebo rozhodnutí přijaté příslušným orgánem podle čl. 4 odst. 4 nebo čl. 5 odst. 4, 6 nebo 7 u soudů těchto členských států (čl. 9 odst. 1 a 2). Tyto postupy se v členských státech, v nichž jsou zavedeny, většinou týkají žalob. Zda jsou tyto postupy „účinné“ nebo specifické pro nařízení, však nelze na základě současných údajů získaných od členských států určit, protože dosud nebylo napadeno žádné rozhodnutí.

4.4 ZVLÁŠTNÍ OPATŘENÍ A SOUVISEJÍCÍ TRANSPARENTNOST (články 5 a 7)

Podle dostupných informací nebyl dosud žádný poskytovatel hostingových služeb považován za vystaveného teroristickému obsahu ve smyslu čl. 5 odst. 4 nařízení. V důsledku toho se požadavek na přijetí zvláštních opatření stanovených v uvedeném článku (zatím) nevztahuje na žádného poskytovatele hostingových služeb.

Přesto lze konstatovat, že podle zpráv o transparentnosti, které poskytli poskytovatelé hostingových služeb, přijalo několik poskytovatelů hostingových služeb opatření týkající se boje proti zneužívání jejich služeb k šíření teroristického obsahu, zejména přijetím zvláštních podmínek a uplatněním dalších ustanovení a opatření k omezení šíření teroristického obsahu. Jak bylo uvedeno výše, podle článku 7 musí poskytovatelé hostingových služeb v tomto ohledu zajistit transparentnost nejen prostřednictvím zpráv o transparentnosti, ale také zahrnutím jasných informací do svých podmínek.

4.5 BEZPROSTŘEDNÍ OHROŽENÍ ŽIVOTA (čl. 14 odst. 5)

Podle čl. 14 odst. 5 nařízení, pokud se poskytovatelé hostingových služeb dozvědí o teroristickém obsahu, jenž obnáší bezprostřední ohrožení života, neprodleně uvědomí orgány příslušné k vyšetřování a stíhání trestných činů v dotčených členských státech. Není-li možné dotčené členské státy určit, poskytovatelé hostingových služeb předají informace Europolu za účelem přijetí vhodných následných opatření.

Do 31. prosince 2023 byla Komise informována o devíti případech, kdy jednotka EU pro oznamování internetového obsahu vytvořená Europolem obdržela informace o teroristickém obsahu, jenž obnášel bezprostřední ohrožení života. Vzhledem k tomu, že čl. 14 odst. 5 nařízení nestanoví povinnost informovat Europol ve všech případech, mohl by být počet oznámení vyšší. Jediným členským státem, který poskytl informace o uplatnění čl. 14 odst. 5, bylo Španělsko. Dne 18. dubna 2023 obdržely španělské orgány od společnosti Amazon oznámení o údajné položce teroristického obsahu, jenž obnášel bezprostřední ohrožení života, na videoherní platformě Twitch. Bylo vyhodnoceno, že obsah neodpovídá podmínkám pro teroristický obsah obnášející bezprostřední ohrožení života ve smyslu nařízení.

[14] Je třeba poznamenat, že poskytnuté informace nemusí být úplné. K získání úplného a zcela aktuálního přehledu o způsobu, jakým členské státy plní požadavek na zajištění dostupnosti účinných prostředků nápravy, by bylo zapotřebí dalších hodnocení.

4.6 SPOLUPRÁCE MEZI POSKYTOVATELI HOSTINGOVÝCH SLUŽEB, PŘÍSLUŠNÝMI ORGÁNY A EUROPOLEM (článek 14)

Jak bylo uvedeno výše, Europol vytvořil platformu nazvanou „PERCI“, která má podporovat provádění nařízení tím, že centralizuje, koordinuje a usnadňuje **předávání příkazů k odstranění a hlášení** ze strany členských států poskytovatelům hostingových služeb. Platforma je v provozu od 3. července 2023. Před plným zprovozněním platformy PERCI zavedl Europol pohotovostní opatření na podporu manuálního předávání příkazů k odstranění, sladění činností, pokud jde o obsah, aby se zabránilo zásahům do probíhajícího vyšetřování, a reakce na krizi v situacích „bezprostředního ohrožení života“.

Platforma PERCI je jednotný systém umožňující spolupráci mezi příslušnými orgány, poskytovateli hostingových služeb a Europolem, jak je stanoveno v článku 14 nařízení, pokud jde o záležitosti, na které se vztahuje nařízení. Konkrétně platforma PERCI:

- je cloudové řešení určené k zajištění bezpečnosti a ochrany dat v cloudu,
- je jednotná platforma pro spolupráci a koordinaci v reálném čase, která podporuje rychlé odstraňování teroristického obsahu,
- usnadňuje proces přezkumu přeshraničních příkazů k odstranění,
- posiluje sladění činností, což je důležité, aby se zabránilo tomu, že příslušný orgán členského státu zašle příkaz k odstranění obsahu, který je předmětem probíhajícího vyšetřování v jiném členském státě,
- umožňuje poskytovatelům hostingových služeb přijímat příkazy k odstranění jednotným a standardizovaným způsobem z jediného kanálu.

Platforma PERCI umožňuje také samostatné předávání hlášení.

V současné době platforma PERCI kromě svého významu v souvislosti s hlášeními (viz 40. bod odůvodnění nařízení) usnadňuje předávání příkazů k odstranění (články 3 a 4), podávání zpráv členskými státy (článek 8) a koordinaci, jakož i sladění činností v případě rozporu s probíhajícími vyšetřováními obsahu, pro který má být zaslán příkaz k odstranění (článek 14). Platforma PERCI v současné době prochází dalším vývojem s cílem podpořit další úkoly vyplývající z nařízení, jako je přezkum přeshraničních příkazů k odstranění (článek 4)[15].

Členské státy potvrdily, že podle článku 14 nařízení:

- příslušné orgány si vyměňují informace, koordinují svou činnost a spolupracují s ostatními příslušnými orgány,
- příslušné orgány si vyměňují informace, koordinují svou činnost a spolupracují s Europolem,

[15] Podrobněji: – články 3 a 4: předávání příkazů k odstranění, – čl. 3 odst. 6 až 8: zpětná vazba poskytovatelů hostingových služeb, – čl. 4 odst. 3 až 7: mechanismus přezkumu, – článek 7: podávání zpráv, – čl. 14 odst. 1: sladění činností, koordinace, zabránění zdvojování úsilí, – čl. 14 odst. 3: bezpečné komunikační cesty, – čl. 14 odst. 4: využívání specializovaného nástroje vytvořeného Europolem, – čl. 14 odst. 5: oznámení týkající se „bezprostředního ohrožení života“, – 40. bod odůvodnění: předávání hlášení.

- jsou zavedeny mechanismy pro posílení spolupráce, které zároveň zabraňují zásahům do vyšetřování probíhajících v jiných členských státech,
- většina členských států považuje platformu PERCI za upřednostňovaný nástroj pro předávání příkazů k odstranění, protože umožňuje koordinaci opatření prostřednictvím sladění činností.

4.7 VLIV NA HLÁŠENÍ

Hlášení teroristického obsahu je dobrovolným nástrojem, který se používal již před přijetím nařízení. Ačkoli nařízení nestanoví pro hlášení žádná zvláštní pravidla, v souladu s jeho 40. bodem odůvodnění nic nebrání členským státům a Europolu, aby hlášení používaly jako nástroj k potírání teroristického obsahu online.

Od svého zřízení v roce 2015 se jednotka EU pro oznamování internetového obsahu v rámci Europolu aktivně podílí na identifikaci teroristického obsahu online a jeho hlášení poskytovatelům hostingových služeb, jakož i na vytváření nástrojů (tj. platforma PERCI a dříve aplikace IRMA[16]), které usnadňují předávání hlášení.

Podle informací poskytnutých Komisi orgány členských států nadále využívají hlášení u některých poskytovatelů hostingových služeb, přičemž mohou zvážit vydání příkazů k odstranění u poskytovatelů hostingových služeb, kteří na hlášení nereagují, nebo z jiných důvodů, jako je naléhavost odstranění obsahu.

4.8 PODPORA MENŠÍCH POSKYTOVATELŮ HOSTINGOVÝCH SLUŽEB PŘI PROVÁDĚNÍ NAŘÍZENÍ

Nařízení obsahuje různé povinnosti pro poskytovatele hostingových služeb. Zatímco velcí poskytovatelé hostingových služeb obvykle disponují technickými možnostmi, kapacitou pro manuální ověřování a znalostmi pro provádění nařízení, malí poskytovatelé mohou mít pro tento účel omezenější finanční, technické a lidské zdroje a odborné znalosti. Současně se menší poskytovatelé hostingových služeb stále častěji stávají terčem nepřátelských subjektů, které zneužívají jejich služeb. To lze také přičíst účinnému úsilí v oblasti moderování obsahu ze strany větších poskytovatelů hostingových služeb. Tento trend svědčí o úspěšnosti opatření týkajících se moderování obsahu, ale také zdůrazňuje potřebu podpořit menší poskytovatele hostingových služeb při zvyšování jejich kapacity a znalostí, aby mohli plnit požadavky nařízení.

V reakci na tento problém vyhlásila Komise výzvu k podávání návrhů v rámci Fondu pro vnitřní bezpečnost na podporu menších poskytovatelů hostingových služeb při provádění nařízení[17].

[16] Aplikaci pro správu hlášení obsahu na internetu (IRMA – Internet Referral Management Application) k podpoře hlášení (označování) nelegálního obsahu poskytovatelům online služeb vytvořil Europol v roce 2016. Zpočátku byl přístup do aplikace IRMA umožněn zaměstnancům Europolu a specializovaným jednotkám (jednotkám pro oznamování internetového obsahu) v sedmi členských státech. Dne 3. července 2023 byla aplikace IRMA nahrazena platformou PERCI.

[17] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/isf/wp-call/2021-2022/call-fiche_isf-2021-ag-tco_en.pdf

Komise vybrala tři projekty[18], aby je podpořila trojím způsobem. Zaprvé informováním a zvyšováním povědomí o pravidlech a požadavcích nařízení, zadruhé vývojem, zaváděním a rozvíjením nástrojů a rámců potřebných k potírání šíření teroristického obsahu online a zatřetí sdílením zkušeností a osvědčených postupů v celém odvětví.

Tyto tři projekty zahájily svou činnost v roce 2023 a již přinesly cenné výsledky. Například projekt FRISCO ve své zprávě o mapování[19] zjistil, že mikroposkytovatelé a malí poskytovatelé hostingových služeb mají obvykle velmi omezené povědomí a znalosti o nařízení, a zdůraznil možné potíže, kterým by mohli čelit při reakci na příkazy k odstranění do jedné hodiny, protože často nemají k dispozici nepřetržité služby. Problémem je nedostatek zdrojů a také navázání komunikace s donucovacími orgány. Více než polovina poskytovatelů hostingových služeb oslovených dodavateli nemoderuje obsah vytvářený uživateli a uvedla, že se na svých platformách nikdy nesetkala s teroristickým obsahem. Pokud se takový obsah objeví na jejich platformách, přijmou tito poskytovatelé hostingových služeb pravděpodobně opatření *ad hoc*.

Prostřednictvím těchto tří projektů jsou malí poskytovatelé hostingových služeb podporováni ve svém úsilí o dodržování pravidel nařízení, a to i zřízením kontaktních míst a zavedením mechanismů pro stížnosti uživatelů.

Kromě toho může být zejména pro menší poskytovatele hostingových služeb relevantní čl. 3 odst. 2 nařízení, který vyžaduje včasné poskytnutí informací o platných postupech a lhůtách poskytovatelům hostingových služeb, kterým dříve nebyl vydán žádný příkaz k odstranění.

4.9 ZÁRUKY ZÁKLADNÍCH PRÁV

Nařízení obsahuje různé záruky k posílení odpovědnosti a transparentnosti opatření přijatých k odstraňování teroristického obsahu online. V tomto ohledu se odkazuje na výše uvedené, zejména na informace o prostředcích nápravy, podávání zpráv a zvláštním mechanismu pro přeshraniční příkazy k odstranění.

Článek 23 nařízení dále vyžaduje, aby Komise v rámci hodnocení nařízení podávala zprávy o fungování a účinnosti ochranných mechanismů, zejména těch, které jsou uvedeny v čl. 4 odst. 4, čl. 6 odst. 3 a v článcích 7 až 11. Tato ochranná opatření se týkají mechanismů stížností, prostředků nápravy a sankcí přijatých a zavedených proti riziku chybného odstranění teroristického obsahu online za účelem ochrany poskytovatelů obsahu a poskytovatelů hostingových služeb. Posouzení fungování a účinnosti ochranných mechanismů bude proto součástí hodnocení podle článku 23.

[18] 1) rámec založený na umělé inteligenci pro podporu mikroposkytovatelů a malých poskytovatelů hostingových služeb v oblasti hlášení a odstraňování teroristického obsahu online (ALLIES); 2) boj proti teroristickému obsahu online (FRISCO) a 3) technologie proti terorismu v Evropě (TATE). Odkaz pro více informací: Financování a výběrová řízení (europa.eu).

[19] Vypracována v období šesti měsíců, které skončilo v květnu 2023. Zpráva je založena na zpětné vazbě od 48 evropských poskytovatelů hostingových služeb, přičemž 33 odpovědí bylo získáno v našem online průzkumu a patnáct v rozhovorech. FRISCO, *D2.1*: *Zpráva o mapování týkající se potřeb a překážek dosažení souladu s předpisy Pochopení potřeb a povědomí malých poskytovatelů a mikroposkytovatelů hostingových služeb v souvislosti s prováděním požadavků nařízení o potírání šíření teroristického obsahu online*, k dispozici na adrese Výstupy | Frisco (friscoproject.eu).

V tomto ohledu je v programu monitorování dle čl. 21 odst. 2 nařízení stanoven rámec ukazatelů pro hodnocení účinků nařízení na základní práva, který bude sloužit jako podklad k hodnocení nařízení.

Program monitorování podpoří posouzení, které bude provedeno v rámci hodnocení a zaměřeno na fungování a účinnost ochranných mechanismů zavedených v souvislosti s nařízením a jejich dopad na základní práva. Tato oblast dopadů odráží dvě oblasti uvedené v článku 23 nařízení: a) fungování a účinnost ochranných mechanismů, zejména těch, které jsou uvedeny v čl. 4 odst. 4, čl. 6 odst. 3 a v článcích 7 až 11, a b) dopad uplatňování tohoto nařízení na základní práva, zejména svobodu projevu a informací, respektování soukromého života a ochranu osobních údajů.

4.10 PŘÍSLUŠNÉ ORGÁNY (článek 13)

Podle článku 13 nařízení musí členské státy zajistit, aby jejich příslušné orgány měly nezbytné pravomoci a dostatečné zdroje k dosažení cílů nařízení a plnění svých povinností, které z něj vyplývají. S cílem zajistit, aby příslušné orgány měly nezbytné pravomoci a dostatečné zdroje, zavedly některé členské státy tato opatření:

- zřízení nových orgánů/ředitelství,
- přidělení dodatečných finančních prostředků a dalších zaměstnanců a
- vytváření nových legislativních rámců.

5. ZÁVĚR

Je nanejvýš důležité, aby byly plně zavedeny všechny nástroje a opatření na úrovni EU, které umožní rychle řešit nelegální obsah šířený online. To platí zejména s ohledem na obrovský rozsah takového nelegálního obsahu, který se šíří v poslední době v souvislosti s útokem Hamásu proti Izraeli.

Nařízení přispívá ke zvýšení veřejné bezpečnosti v celé Unii tím, že předchází tomu, aby poskytovatele hostingových služeb působící na vnitřním trhu využívali teroristé k šíření svých myšlenek za účelem zastrašování, radikalizace, náboru a usnadnění teroristických útoků.

Po zahájení řízení o nesplnění povinnosti v lednu 2023 bylo **dosaženo pokroku**. Ke dni 31. prosince 2023 určilo 23 členských států příslušné orgány podle čl. 12 odst. 1, jak je uvedeno v online rejstříku, což povede k systematičtějšímu využívání opatření a nástrojů stanovených v nařízení. Kromě toho bylo ke dni 21. prosince 2023 uzavřeno 11 z 22 případů porušení povinnosti zahájených v lednu 2023. Komise vybízí zbývající členské státy, aby urychleně učinily nezbytné kroky k určení příslušných orgánů dle čl. 12 odst. 1 a plnění povinností dle čl. 12 odst. 2 a 3 a čl. 18 odst. 1.

Celkově členské státy hlásí, že příkazy k odstranění jsou za podpory Europolu předávány poskytovatelům hostingových služeb bez obtíží. Na základě informací obdržených od členských států a Europolu bylo od vstupu nařízení v platnost předáno nejméně 349 **příkazů k odstranění teroristického obsahu**. V deseti případech jeden poskytovatel hostingových služeb neodstranil

teroristický obsah / nezablokoval k němu přístup v maximální lhůtě jedné hodiny stanovené nařízením.

Podle informací získaných od členských států a Europolu se od doby, kdy nařízení vstoupilo v platnost, zvýšila schopnost reakce na hlášení teroristického obsahu, přestože nařízení v tomto ohledu neobsahuje žádná pravidla. Kromě toho Europol obdržel od poskytovatelů hostingových služeb v devíti případech informace o teroristickém obsahu obnášejícím bezprostřední ohrožení života podle čl. 14 odst. 5.

Účinnější komunikační cesty a postupy jsou zavedeny zejména od spuštění platformy PERCI dne 3. července 2023, které vedlo k systematičtějšímu přístupu k předávání příkazů k odstranění, přičemž platforma PERCI se využívá také k předávání vysokého počtu hlášení. Členské státy a Europol vyjádřily očekávání, že zavedení platformy PERCI bude přínosem pro využívání těchto nástrojů v boji proti teroristickému obsahu online.

Na tomto základě Komise hodnotí, že nařízení mělo na omezení šíření teroristického obsahu online celkově **pozitivní dopad**. Nicméně v deseti případech ze 349 překročil cílový poskytovatel hostingových služeb maximální lhůtu pro odstranění teroristického obsahu nebo zablokování přístupu k němu, která dle nařízení činí jednu hodinu.

Komise aktivně podporuje členské státy a poskytovatele hostingových služeb, mimo jiné prostřednictvím technických seminářů pořádaných před vstupem nařízení v platnost i po něm. Poslední se uskutečnil dne 24. listopadu 2023. Komise rovněž podporuje zejména menší poskytovatele hostingových služeb, aby zajistila plné a urychlené uplatňování nařízení, a pomáhá jim při řešení problémů, jimž dosud čelili.

Komise bude monitorovat provádění a uplatňování nařízení i nadále. Komise bude pečlivě monitorovat výkonnost nástrojů stanovených v nařízení prostřednictvím programu monitorování, který bude podkladem pro hodnocení nařízení podle článku 23.