EURÓPSKA
KOMISIA

V Bruseli 14. 2. 2024
COM(2024) 64 final

SPRÁVA KOMISIE EURÓPSKEMU PARLAMENTU A RADE

o vykonávaní nariadenia (EÚ) 2021/784 o riešení šírenia teroristického obsahu online

{SWD(2024) 36 final}

1. ZHRNUTIE

Nariadenie (EÚ) 2021/784 o riešení šírenia teroristického obsahu online tvorí právny rámec na európskej úrovni, ktorý slúži členským štátom na ochranu obyvateľov pred tým, aby boli vystavení teroristickému materiálu online. Cieľom nariadenia je zabezpečiť hladké fungovanie digitálneho jednotného trhu riešením zneužívania hostingových služieb na verejné šírenie teroristického obsahu online. Jeho cieľom je zabrániť tomu, aby teroristi využívali internet na šírenie svojich odkazov, ktorými zastrašujú, radikalizujú, uskutočňujú nábor a uľahčujú teroristické útoky. Je to obzvlášť dôležité v súčasnej situácii, keď čelíme konfliktu a nestabilite s dosahom na bezpečnosť Európy. V dôsledku ruskej útočnej vojny proti Ukrajine a teroristického útoku, ktorý spáchal Hamas proti Izraelu 7. októbra 2023, stúplo množstvo teroristického obsahu, ktorý sa šíri na internete.

Nadobudnutím účinnosti aktu o digitálnych službách 16. novembra 2022 sa ešte viac posilnil regulačný rámec na riešenie nezákonného obsahu online. Aktom o digitálnych službách sa upravujú povinnosti digitálnych služieb pôsobiacich ako sprostredkovatelia, pokiaľ ide o ich úlohu spájať spotrebiteľov s obsahom, so službami a s tovarom, čím sa lepšie chránia používatelia v online priestore a prispieva k bezpečnejšiemu online prostrediu.

Nariadenie o riešení šírenia teroristického obsahu online nadobudlo účinnosť 7. júna 2022. Podľa článku 22 nariadenia Komisia predloží Európskemu parlamentu a Rade správu o uplatňovaní nariadenia (ďalej len „správa o vykonávaní“).

Táto správa o vykonávaní vychádza z posúdenia informácií, ktoré poskytli členské štáty, Europol a poskytovatelia hostingových služieb v súlade s povinnosťami stanovenými v nariadení. Na základe tohto posúdenia možno kľúčové zistenia súvisiace s vykonávaním nariadenia zhrnúť takto:

- K 31. decembru 2023 **23 členských štátov** určilo príslušný(-é) orgán(-y) s právomocou vydávať príkazy na odstránenie, ako sa stanovuje v nariadení[1]. Zoznam orgánov členských štátov je dostupný na webovom sídle Komisie a pravidelne sa aktualizuje[2].

- K 31. decembru 2023 Komisia dostala informácie o najmenej **349 príkazoch na odstránenie teroristického obsahu**, ktoré vydali príslušné orgány šiestich členských štátov (Španielsko, Rumunsko, Francúzsko, Nemecko, Česko a Rakúsko), čo vo väčšine prípadov viedlo k prijatiu rýchlych následných opatrení poskytovateľmi hostingových služieb, ktorými odstránili teroristický obsah alebo zablokovali prístup k nemu. Nasvedčuje to tomu, že nástroje stanovené v nariadení sa začínajú používať a úspešne zabezpečujú rýchle odstránenie teroristického obsahu poskytovateľmi hostingových

[1] Online register zriadený Komisiou podľa článku 12 ods. 4 nariadenia so zoznamom príslušných orgánov uvedených v článku 12 ods. 1 a kontaktných miest jednotlivých príslušných orgánov určených alebo zriadených podľa článku 12 ods. 2. Pravidelne sa aktualizuje na základe oznámení prijatých od členských štátov. Zoznam príslušných vnútroštátnych orgánov a kontaktných miest (europa.eu).
[2] Zoznam príslušných vnútroštátnych orgánov a kontaktných miest.

služieb podľa článku 3 ods. 3. Podľa informácií, ktoré dostala Komisia, tieto príkazy na odstránenie neboli napadnuté.

- **Koordinácia** medzi príslušnými orgánmi členských štátov a Europolom, najmä jednotkou Europolu pre nahlasovanie internetového obsahu (EU IRU), **funguje dobre** pri uplatňovaní nariadenia, predovšetkým pri spracúvaní príkazov na odstránenie.
- Nástroj Europolu „**PERCI**“[3] bol uvedený do prevádzky 3. júla 2023. Tento nástroj úspešne využili niektoré členské štáty na zaslanie príkazov na odstránenie, ako aj na nahlasovanie[4]. Španielske, nemecké, rakúske, francúzske a české príslušné orgány využili nástroj na zaslanie príkazov na odstránenie. Celkovo bolo spracovaných prinajmenšom 14 615 nahlásení v nástroji PERCI od jeho uvedenia do prevádzky 3. júla 2023 až do 31. decembra 2023.
- Hoci nariadenie neobsahuje žiadne konkrétne opatrenia týkajúce sa nahlasovania, podľa informácií, ktoré dostala Komisia, sa od nadobudnutia účinnosti nariadenia takisto **zvýšila schopnosť** poskytovateľov hostingových služieb **reagovať na nahlásenia**.
- Podľa poznatkov Komisie do 31. decembra 2023 sa v prípade žiadneho z poskytovateľov hostingových služieb nezistilo, že bol vystavený teroristickému obsahu, ako sa vymedzuje v článku 5 ods. 4 nariadenia. Toto zistenie je predpokladom uplatnenia osobitných opatrení uvedených v danom článku. Podľa správ o transparentnosti, ktoré predložili poskytovatelia hostingových služieb, však poskytovatelia hostingových služieb prijali opatrenia **na riešenie zneužívania svojich služieb** na šírenie teroristického obsahu, najmä prostredníctvom prijatia osobitných zmluvných podmienok a uplatňovania iných ustanovení a opatrení na obmedzenie šírenia teroristického obsahu.
- Poskytovatelia hostingových služieb okrem toho prijali opatrenia na oznamovanie **bezprostredného ohrozenia života** v zmysle článku 14 ods. 5 nariadenia.

Pokiaľ ide o **menších poskytovateľov hostingových služieb**, Komisia v roku 2021 uverejnila výzvu na predkladanie návrhov s cieľom podporiť ich pri vykonávaní nariadenia. Komisia v roku 2022 vybrala tri projekty (pozri oddiel 4.8), ktoré sa začali vykonávať v roku 2023 a už priniesli isté výsledky pri poskytovaní podpory malým podnikom, aby dosiahli súlad s nariadením.

Komisia začala konania o nesplnení povinnosti proti 22 členským štátom z dôvodu, že neurčili príslušné orgány podľa článku 12 ods. 1 nariadenia, a z dôvodu nesplnenia ich povinností podľa článku 12 ods. 2 a 3 a článku 18 ods. 1, a to tak, že im 26. januára 2023 zaslala **formálne výzvy**[5]. Po začatí týchto konaní o nesplnení povinnosti sa zvýšil počet členských štátov, ktoré oznámili príslušné orgány zodpovedné za vybavovanie príkazov na odstránenie, ako sa uvádza

[3] PERCI (*Plateforme Européenne de Retraits des Contenus illégaux sur Internet*) je platforma na odstraňovanie nezákonného obsahu online, ktorú vyvinul a spravuje Europol. Podporuje vykonávanie nariadenia tým, že okrem iných funkcií poskytuje poskytovateľom hostingových služieb technické riešenie na spracúvanie nahlásení a príkazov na odstránenie.

[4] Nahlasovanie je mechanizmus, ktorý upozorňuje poskytovateľov hostingových služieb, aby dobrovoľne posúdili zlučiteľnosť daného obsahu s vlastnými zmluvnými podmienkami. V nariadení (odôvodnení 40) sa uvádza, že nahlasovanie sa ukázalo ako účinný prostriedok a popri príkazoch na odstránenie by malo zostať k dispozícii.

[5] Pozri tlačovú správu: Teroristický obsah online (europa.eu).

v informáciách uverejnených v online registri[6]. Navyše 11 prípadov nesplnenia povinnosti začatých v januári 2023 bolo do 21. decembra 2023 uzavretých[7].

Na základe informácií získaných od členských štátov a Europolu, ako aj informácií od poskytovateľov hostingových služieb Komisia dospela k záveru, že uplatňovanie nariadenia malo **pozitívny vplyv** na obmedzenie šírenia teroristického obsahu online.

2. SÚVISLOSTI

Nariadenie nadobudlo účinnosť 7. júna 2022. Jeho cieľom je zabezpečiť hladké fungovanie digitálneho jednotného trhu riešením zneužívania hostingových služieb na verejné šírenie teroristického obsahu online. Členským štátom poskytuje cielené nástroje vo forme príkazov na odstránenie, ktoré slúžia na riešenie šírenia teroristického obsahu online, a členským štátom umožňuje požiadať poskytovateľov hostingových služieb všetkých veľkostí, aby prijali osobitné opatrenia na ochranu svojich služieb pred zneužívaním teroristickými aktérmi pri vystavení teroristickému obsahu.

Okrem toho sa tým, že akt o digitálnych službách nadobudol účinnosť 16. novembra 2022, rozširuje regulačné prostredie prostredníctvom horizontálnych právnych predpisov so širokým rozsahom pôsobnosti. Ich cieľom je zabezpečiť bezpečnejší digitálny priestor pre spotrebiteľov, účinné opatrenia na boj proti nezákonnému obsahu a transparentnejšie podmienky služby. Akt o digitálnych službách poskytuje Komisii rozsiahle právomoci v oblasti dohľadu, vyšetrovania a presadzovania práva, aby mohla prijímať opatrenia zamerané na veľmi veľké online platformy a vyhľadávače. Tieto opatrenia zahŕňajú žiadosti o informácie a vyšetrovanie činností spoločností týkajúcich sa moderovania obsahu s možnosťou uloženia pokút.

Akt o digitálnych službách umožňuje riešiť všetky formy nezákonného obsahu, vďaka čomu Komisia môže vyzývať platformy, aby poskytli údaje preukazujúce, že plnia svoje vlastné záväzky v oblasti odstraňovania obsahu. Popritom nariadenie o teroristickom obsahu online poskytuje ešte silnejší nástroj proti tejto konkrétnej forme nezákonného obsahu s právnou povinnosťou odstrániť obsah do jednej hodiny od doručenia príkazu na odstránenie, ako aj účinné sankčné mechanizmy.

Ako sa zdôrazňuje v správach Europolu o situácii a trendoch v oblasti terorizmu (TE-SAT)[8] zverejnených v uplynulých rokoch, teroristi intenzívne využívajú internet na šírenie svojich odkazov, ktorými zastrašujú, radikalizujú, uskutočňujú nábor a uľahčujú teroristické útoky. Hoci dobrovoľné opatrenia a nezáväzné odporúčania úspešne napomáhali pri znižovaní dostupnosti teroristického obsahu online, obmedzenia vrátane malého počtu poskytovateľov hostingových služieb, ktorí prijali dobrovoľné mechanizmy[9], ako aj fragmentácia procesných pravidiel v členských štátoch obmedzili účinnosť a efektívnosť spolupráce medzi členskými štátmi

[6] Zoznam príslušných vnútroštátnych orgánov a kontaktných miest (europa.eu). Online register obsahuje informácie o 23 orgánoch členských štátov príslušných na vydávanie príkazov na odstránenie podľa článku 12 ods. 1 písm. a).
[7] Fínsko, Malta, Česko, Dánsko, Rumunsko, Švédsko, Lotyšsko, Španielsko, Litva, Rakúsko a Slovensko.
[8] TE-SAT Europolu 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] Európska komisia, 2018, Posúdenie vplyvu priložené k návrhu nariadenia o predchádzaní šíreniu teroristického obsahu online, SWD(2018) 408 final, navštívené 4. 5. 2023 na adrese: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN.

a poskytovateľmi hostingových služieb a viedli k potrebe zaviesť regulačné opatrenia[10]. Účinné uplatňovanie nariadenia je preto kľúčom k riešeniu šírenia teroristického obsahu online. Komisia aktívne podporuje príslušné vnútroštátne orgány v tomto procese.

Podľa článku 22 nariadenia bola Komisia povinná predložiť Európskemu parlamentu a Rade správu o uplatňovaní nariadenia (ďalej len „správa o vykonávaní“) do 7. júna 2023, a to na základe informácií poskytnutých členskými štátmi, ktoré zase čiastočne vychádzali z informácií od poskytovateľov hostingových služieb (článok 21). Na jednej strane je príčinou oneskoreného predloženia správy o vykonávaní oneskorené zaslanie kľúčových informácií Komisii zo strany členských štátov a poskytovateľov hostingových služieb. Na druhej strane sa považovalo za dôležité zohľadniť v správe o vykonávaní používanie nástroja PERCI, ktorý bol uvedený do prevádzky 3. júla 2023 a odvtedy sa používa na spracovávanie príkazov na odstránenie podľa nariadenia.

Výlučným cieľom tejto správy o vykonávaní je poskytnúť vecný prehľad relevantných záležitostí týkajúcich sa uplatňovania nariadenia. Nezahŕňa žiaden výklad nariadenia a nevyjadruje sa v ňom názor na výklad či iné opatrenia prijaté v rámci uplatňovania nariadenia.

V súlade s článkom 21 ods. 2 nariadenia mala Komisia povinnosť do toho istého dátumu (7. júna 2023) stanoviť podrobný program na monitorovanie výstupov, výsledkov a vplyvov nariadenia. Konkrétne v programe monitorovania by sa mali stanoviť ukazovatele, spôsob získavania údajov a ďalších potrebných dôkazov, ako aj interval ich získavania. Tento program je stanovený v sprievodnom pracovnom dokumente útvarov Komisie. Špecifikujú sa v ňom kroky, ktoré má podniknúť Komisia a členské štáty pri získavaní a analýze údajov a ďalších dôkazov na monitorovanie pokroku a vplyvu nariadenia a na účely hodnotenia nariadenia podľa článku 23.

3. CIEĽ A METODIKA SPRÁVY

Cieľom tejto správy je posúdiť uplatňovanie nariadenia a jeho doterajší vplyv na obmedzenie šírenia teroristického obsahu online. To zahŕňa kroky podniknuté členskými štátmi a poskytovateľmi hostingových služieb, napríklad zmeny podmienok poskytovania služieb a komunitných usmernení a ich plnenie príkazov na odstránenie či schopnosť reagovať na ne.

Komisia na tento účel zhromaždila informácie od členských štátov, jednotky Europolu pre nahlasovanie internetového obsahu (EU IRU) a poskytovateľov hostingových služieb vrátane informácií uvedených v správach o transparentnosti a monitorovaní podľa článkov 7, 8 a 21 nariadenia. Informácie podľa článkov 8 a 21 získala od 18 členských štátov. Informácie o krokoch, ktoré podnikli poskytovatelia hostingových služieb, boli získané prostredníctvom ich výročných správ o transparentnosti, Europolu a priamou dobrovoľnou komunikáciou s útvarmi Komisie. Táto správa o vykonávaní zahŕňa informácie, ktoré Komisia získala do 31. decembra 2023.

Povinnosti týkajúce sa monitorovania a transparentnosti (články 21, 7 a 8)

Na vypracovanie správy o vykonávaní podľa článku 21 ods. 1 nariadenia sú členské štáty povinné získavať informácie od svojich príslušných orgánov a poskytovateľov hostingových služieb, ktorí

[10] Tamže.

patria do ich právomoci, a každý rok ich do 31. marca zaslať Komisii. Medzi ne patria informácie o krokoch, ktoré podnikli v súlade s nariadením počas predošlého kalendárneho roka. V článku 21 ods. 1 sa uvádza druh informácií, ktoré by členské štáty mali získavať o krokoch podniknutých na dosiahnutie súladu s nariadením, ako sú podrobné informácie o príkazoch na odstránenie, počet žiadostí o prístup k obsahu na umožnenie vyšetrovania, konania vo veci sťažnosti, správne a súdne preskúmania.

Podľa článku 7 ods. 1 nariadenia poskytovatelia hostingových služieb vo svojich zmluvných podmienkach jasne stanovia svoju politiku riešenia šírenia teroristického obsahu vrátane prípadného relevantného vysvetlenia fungovania osobitných opatrení.

Navyše podľa článku 7 ods. 2 nariadenia poskytovateľ hostingových služieb, ktorý v určitom kalendárnom roku podnikol kroky proti šíreniu teroristického obsahu alebo ktorému sa uložila povinnosť podniknúť takéto kroky podľa tohto nariadenia, zverejní správu o transparentnosti týkajúcu sa týchto krokov v danom roku. Táto správa by sa mala zverejniť do 1. marca nasledujúceho roka.

V článku 7 ods. 3 nariadenia sa stanovujú minimálne informácie, ktoré by tieto správy o transparentnosti mali obsahovať, ako sú napríklad opatrenia prijaté v súvislosti s identifikáciou teroristického obsahu a so znemožnením prístupu k nemu, počet odstránených položiek a/alebo počet prípadov obnoveného obsahu a výsledky sťažností.

V článku 8 nariadenia sa uvádza, že určené príslušné orgány členských štátov uverejňujú výročné správy o transparentnosti týkajúce sa ich činností podľa nariadenia. V článku 8 ods. 1 sa uvádza minimum informácií, ktoré by mali tieto správy obsahovať[11].

K 31. decembru 2023 Komisii zaslalo 18 členských štátov informácie o krokoch, ktoré podnikli v súlade s nariadením, pričom 23 členských štátov určilo orgán(-y) s právomocou vydávať príkazy na odstránenie, ako sa stanovuje v nariadení.

4. KONKRÉTNE BODY POSÚDENIA

4.1. PRÍKAZY NA ODSTRÁNENIE (článok 3)

K 31. decembru 2023 bola Komisia celkovo informovaná o najmenej 349 príkazoch na odstránenie, ktoré príslušné orgány Španielska, Rumunska, Francúzska, Nemecka, Rakúska a Česka zaslali poskytovateľom aplikácií 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.

Španielsky príslušný orgán (*CITCO – Centro de Inteligencia contra el Terrorismo y el Crimen Organizado*) zaslal 62 príkazov na odstránenie, zatiaľ čo rumunský príslušný orgán (*ANCOM – Autoritatea Națională pentru Administrare și Reglementare în Comunicații*) zaslal dva príkazy na odstránenie a francúzsky príslušný orgán (*OCLCTIC – L'Office central de lutte contre*

[11] Pozri znenie nariadenia (EÚ) 2021/784, článok 8 ods. 1, https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32021R0784.

la criminalité liée aux technologies de l'information et de la communication) zaslal 26 príkazov na odstránenie. Od teroristického útoku, ktorý spáchal Hamas proti Izraelu, nemecký príslušný orgán (*BKA – Bundeskriminalamt*) zaslal 249 príkazov na odstránenie.

Španielsky príslušný orgán zaslal 62 príkazov na odstránenie: 18 pred uvedením nástroja PERCI do prevádzky a 44 prostredníctvom nástroja PERCI. Poskytol podrobný opis zaslania prvých príkazov na odstránenie a následných opatrení, čo má veľký význam pre lepšie pochopenie dôsledkov a účinkov nariadenia.

Prvé dva príkazy na odstránenie vydal španielsky príslušný orgán 24. apríla 2023.[12] Išlo o dva prípady teroristického obsahu, jeden sa týkal pravicového terorizmu a druhý sa týkal džihádizmu. Obsahom, na ktorý sa vzťahoval prvý príkaz na odstránenie, bol dokument vo formáte PDF zverejnený s neobmedzeným prístupom na platforme Telegram, v ktorom sa vyjadrovala podpora teroristickému násiliu a velebili pravicové teroristické útoky. Teroristickým obsahom, na ktorý sa vzťahoval druhý príkaz na odstránenie, bolo video s obrázkami džihádistov z teroristickej organizácie tzv. Islamský štát v boji, ktoré bolo nahraté na platformu Internet Archive. Tieto dva prípady s takýmto obsahom boli odstránené z oboch platforiem za menej ako hodinu, a teda v súlade s článkom 3 ods. 3 nariadenia. V posúdení poskytnutom španielskym príslušným orgánom sa vysvetlilo, že si zvolil príkaz na odstránenie namiesto nahlásenia z dvoch hlavných dôvodov: zabezpečenie súladu s požiadavkami v nariadení týkajúcimi sa príkazov na odstránenie a naliehavosť. Španielsky príslušný orgán následne zaslal ďalšie príkazy na odstránenie.

Španielsky orgán zdôraznil problémy spojené s používaním webového formulára na prijímanie príkazov na odstránenie jedným poskytovateľom hostingových služieb (Meta) namiesto toho, aby poskytol priame kontaktné miesto. Tento webový formulár takisto viedol k problémom s komunikáciou s príslušným orgánom členského štátu, kde sa nachádza hlavné miesto podnikateľskej činnosti poskytovateľa hostingových služieb.

Francúzsky príslušný orgán vydal 13. júla 2023 prvý príkaz na odstránenie platforme na zdieľanie (Justpaste.it), ktorá teroristický obsah odstránila do jednej hodiny. Cieleným obsahom bola propaganda al-Káidy, konkrétnejšie mediálneho orgánu Rikan Ka Mimber z indickej vetvy Al Qaeda Indian Subcontinent (AQIS). Na platforme Europolu PERCI bolo potvrdené úplné odstránenie obsahu.

Nemecký príslušný orgán vydal šesť príkazov na odstránenie 16. októbra 2023, 16 príkazov na odstránenie 18. októbra 2023 a päť príkazov na odstránenie 24. októbra 2023, pričom sa zameral na propagandu hnutia Hamas a Palestínskeho islamského džihádu. Prístup k obsahu bol v EÚ zablokovaný v súlade s článkom 3 ods. 3 nariadenia. Nemecký príslušný orgán najprv obsah nahlásil a následne vydal príkazy na odstránenie, keďže nahlásenia ostali bez reakcie. Po útoku Hamasu 7. októbra 2023 nemecký príslušný orgán zaslal 249 príkazov na odstránenie, prevažne platforme Telegram.[13]

[12] Ministerio del Interior | El CITCO culmina la retirada de Internet de dos contenidos que alentaban al terrorismo.
[13] Podľa informácií, ktoré boli Komisii dostupné.

Český príslušný orgán a rakúsky príslušný orgán vydali platforme X dva príkazy na odstránenie a platforme Telegram osem príkazov na odstránenie.

Pokiaľ ide o používanie webového formulára na prijímanie príkazov na odstránenie jedným poskytovateľom hostingových služieb, španielske orgány uviedli dva problémy: 1. v kontexte článku 3 ods. 2 nariadenia webový formulár príslušným orgánom členských štátov neumožňuje zaslať informácie o uplatniteľných postupoch a lehotách pred vydaním prvého príkazu na odstránenie poskytovateľovi hostingových služieb; 2. v kontexte článku 4 ods. 1 webový formulár neumožňuje súčasne predložiť kópiu príkazu na odstránenie príslušnému orgánu členského štátu, v ktorom má poskytovateľ hostingových služieb svoje hlavné miesto podnikateľskej činnosti, a právnemu zástupcovi poskytovateľa hostingových služieb.

4.2. CEZHRANIČNÉ PRÍKAZY NA ODSTRÁNENIE (článok 4)

V prípade prvých dvoch príkazov na odstránenie vydaných v apríli 2023 španielsky príslušný orgán nemohol zaslať kópie orgánu členského štátu, v ktorom má poskytovateľ hostingových služieb svoje hlavné miesto podnikateľskej činnosti, alebo jeho právnemu zástupcovi, pretože v tom čase ani jeden z týchto dvoch poskytovateľov hostingových služieb nemal hlavné miesto podnikateľskej činnosti ani neurčil právneho zástupcu v EÚ. V prípade nasledujúcich príkazov na odstránenie španielsky príslušný orgán zaslal kópie príslušnému orgánu členského štátu, v ktorom mal poskytovateľ hostingových služieb svoje hlavné miesto podnikateľskej činnosti alebo určil svojho právneho zástupcu.

Členské štáty oznámili, že zasielanie príkazov na odstránenie poskytovateľom hostingových služieb usadeným v tretích krajinách, ktorí si ešte nesplnili povinnosť určiť právneho zástupcu v EÚ, predstavovalo problém. V tejto súvislosti Komisia podporila členské štáty pri zabezpečovaní splnenia povinnosti poskytovateľov hostingových služieb určiť právneho zástupcu v EÚ a zriadiť kontaktné miesto (článok 15 ods. 1 nariadenia), napríklad e-mailovú adresu, aby sa zaistilo prijatie okamžitých krokov. Navyše Komisia pripomenula poskytovateľom hostingových služieb ich povinnosti na rôznych fórach, aj na internetovom fóre EÚ.

Podľa informácií, ktoré boli Komisii dostupné, žiadny príslušný orgán členského štátu, v ktorom má poskytovateľ hostingových služieb svoje hlavné miesto podnikateľskej činnosti, doteraz neskontroloval príkaz na odstránenie podľa článku 4 nariadenia s cieľom zistiť, či závažným alebo zjavným spôsobom neporušuje nariadenie alebo základné práva a slobody, keďže ešte nebola predložená žiadna odôvodnená žiadosť o kontrolu. V dôsledku toho dosiaľ žiaden orgán nezistil, že by niektorý príkaz na odstránenie daným spôsobom porušoval uvedené nariadenie alebo základné práva.

Žiadny poskytovateľ hostingových služieb doteraz neobnovil obsah (alebo prístup k nemu), na ktorý sa vzťahoval príkaz na odstránenie, na základe kontroly v súlade s článkom 4 nariadenia, pretože k takejto kontrole a žiadostiam o obnovenie ešte nedošlo. Preto nie sú k dispozícii žiadne informácie o zvyčajnej dĺžke trvania obnovenia obsahu alebo opätovného umožnenia prístupu k nemu ani o „potrebných opatreniach“ prijatých poskytovateľmi hostingových služieb na obnovenie obsahu alebo opätovné umožnenie prístupu k nemu.

4.3. PROSTRIEDKY NÁPRAVY (článok 9)

Podľa informácií, ktoré boli Komisii dostupné, poskytovatelia hostingových služieb dosiaľ nenapadli príkazy na odstránenie alebo rozhodnutia podľa článku 5 ods. 4 na príslušných súdoch. Jeden poskytovateľ hostingových služieb však vyhlásil, že príkaz na odstránenie nie je možné vykonať.

Podľa informácií poskytnutých členskými štátmi[14] má aspoň dvanásť členských štátov zavedené „účinné postupy“, ktoré umožňujú poskytovateľom hostingových služieb a poskytovateľom obsahu napadnúť vydaný príkaz na odstránenie a/alebo rozhodnutie prijaté podľa článku 4 ods. 4 alebo článku 5 ods. 4, 6 alebo 7 na súdoch daných členských štátov príslušného orgánu (článok 9 ods. 1 a 2). V členských štátoch, ktoré majú tieto postupy zavedené, takéto postupy zväčša odkazujú na žaloby. To, či sú tieto postupy „účinné“ alebo špecifické pre nariadenie, sa však nedá zistiť na základe súčasných údajov získaných od členských štátov, keďže dosiaľ nebolo napadnuté žiadne rozhodnutie.

4.4. OSOBITNÉ OPATRENIA A SÚVISIACA TRANSPARENTNOSŤ (články 5 a 7)

Podľa dostupných informácií žiaden poskytovateľ hostingových služieb nebol doteraz vystavený teroristickému obsahu v zmysle článku 5 ods. 4 nariadenia. Vzhľadom na to sa požiadavka prijať osobitné opatrenia stanovené v danom článku (zatiaľ) neuplatňuje na žiadneho poskytovateľa hostingových služieb.

Podľa správ o transparentnosti, ktoré predložili poskytovatelia hostingových služieb, možno však skonštatovať, že viacerí poskytovatelia hostingových služieb prijali opatrenia na riešenie zneužívania svojich služieb na šírenie teroristického obsahu, najmä prijatie osobitných zmluvných podmienok a uplatňovanie ďalších ustanovení a opatrení na obmedzenie šírenia teroristického obsahu. Ako už bolo uvedené, podľa článku 7 poskytovatelia hostingových služieb musia v tomto ohľade zabezpečiť transparentnosť nielen prostredníctvom správ o transparentnosti, ale aj zahrnutím jasných informácií vo svojich zmluvných podmienkach.

4.5. BEZPROSTREDNÉ OHROZENIE ŽIVOTA (článok 14 ods. 5)

V článku 14 ods. 5 nariadenia sa uvádza, že ak sa poskytovatelia hostingových služieb dozvedia o teroristickom obsahu, s ktorým sa spája bezprostredné ohrozenie života, bezodkladne informujú orgány príslušné na vyšetrovanie a stíhanie trestných činov v dotknutých členských štátoch. Ak nie je možné dotknutý členský štát identifikovať, poskytovateľ hostingových služieb zašle informácie Europolu, aby podnikol vhodné nadväzné kroky.

K 31. decembru 2023 bola Komisia informovaná o deviatich prípadoch, keď jednotka EÚ pre nahlasovanie internetového obsahu zriadená Europolom dostala informácie o teroristickom obsahu, s ktorým sa spája bezprostredné ohrozenie života. Keďže z článku 14 ods. 5 nariadenia nevyplýva povinnosť informovať Europol o všetkých prípadoch, počet oznámení mohol byť vyšší.

[14] Treba poznamenať, že poskytnuté informácie nie sú nevyhnutné úplné. Na získanie úplného a najaktuálnejšieho prehľadu o spôsobe, akým členské štáty uplatnili požiadavku zabezpečiť dostupnosť účinných postupov nápravy, by boli potrebné ďalšie posúdenia.

Jediný členský štát, ktorý poskytol informácie o uplatňovaní článku 14 ods. 5, bolo Španielsko. Španielske orgány dostali 18. apríla 2023 oznámenie od spoločnosti Amazon o údajnom teroristickom obsahu, ktorý zahŕňa bezprostredné ohrozenie života, na platforme s videohrami Twitch. Usúdilo sa, že obsah nezodpovedá podmienkam teroristického obsahu, ktorý zahŕňa bezprostredné ohrozenie života, v zmysle nariadenia.

4.6. SPOLUPRÁCA MEDZI POSKYTOVATEĽMI HOSTINGOVÝCH SLUŽIEB, PRÍSLUŠNÝMI ORGÁNMI A EUROPOLOM (článok 14)

Ako už bolo uvedené, Europol vytvoril platformu s názvom „PERCI“ na podporu vykonávania nariadenia centralizáciou, koordináciou a uľahčením **zasielania príkazov na odstránenie a nahlásení** členskými štátmi poskytovateľom hostingových služieb. Platforma je v prevádzke od 3. júla 2023. Pred úplným sprevádzkovaním platformy PERCI Europol zaviedol opatrenia pre prípad nepredvídaných udalostí na podporu manuálneho zasielania príkazov na odstránenie, predchádzania konfliktu záujmov, pokiaľ ide o obsah, s cieľom zabrániť zasahovaniu do prebiehajúcich vyšetrovaní a reakcie na krízy v situáciách „bezprostredného ohrozenia života“.

PERCI je jednotný systém, ktorý umožňuje spoluprácu medzi príslušnými orgánmi, poskytovateľmi hostingových služieb a Europolom, ako sa stanovuje v článku 14 nariadenia v súvislosti s otázkami, na ktoré sa nariadenie vzťahuje. Konkrétnejšie, PERCI:

- predstavuje cloudové riešenie navrhnuté s cieľom zaistiť bezpečnosť a ochranu údajov v cloude,
- je jednotnou platformou pre komunikáciu a koordináciu založenú na spolupráci v reálnom čase, ktorá podporuje rýchle odstraňovanie teroristického obsahu,
- uľahčuje proces kontroly cezhraničných príkazov na odstránenie,
- posilňuje predchádzanie konfliktu záujmov, čo je dôležité na to, aby sa zabránilo tomu, že príslušný orgán členského štátu zašle príkaz na odstránenie zameraný na obsah, ktorý je predmetom prebiehajúceho vyšetrovania v inom členskom štáte,
- umožňuje poskytovateľom hostingových služieb prijímať príkazy na odstránenie jednotným a štandardizovaným spôsobom z jediného kanálu.

PERCI navyše umožňuje nahlasovanie.

V súčasnosti okrem jej významu v súvislosti s nahlasovaním (pozri odôvodnenie 40 nariadenia) platforma PERCI uľahčuje zasielanie príkazov na odstránenie (články 3 a 4), podávanie správ členskými štátmi (článok 8) a koordináciu, ako aj predchádzanie konfliktu záujmov v prípade konfliktu záujmov s prebiehajúcimi vyšetrovaniami, pokiaľ ide o obsah, na ktorý je príkaz na odstránenie zameraný (článok 14). Momentálne prebieha ďalší vývoj platformy PERCI, aby sa

podporili dodatočné úlohy vyplývajúce z nariadenia, ako je kontrola cezhraničných príkazov na odstránenie (článok 4)[15].

Členské štáty v súlade s článkom 14 nariadenia potvrdili:

- príslušné orgány si vymieňajú informácie, koordinujú sa a spolupracujú s ostatnými príslušnými orgánmi,
- príslušné orgány si vymieňajú informácie, koordinujú sa a spolupracujú s Europolom,
- sú zavedené mechanizmy na zlepšenie spolupráce, pričom sa nezasahuje do vyšetrovaní, ktoré prebiehajú v iných členských štátoch,
- väčšina členských štátov uprednostňuje používať na zasielanie príkazov na odstránenie nástroj PERCI, keďže umožňuje koordináciu postupu s tým, že predchádza konfliktu záujmov.

4.7. VPLYV NA NAHLASOVANIE

Nahlasovanie teroristického obsahu je dobrovoľný nástroj, ktorý sa používal už pred prijatím nariadenia. Hoci nariadenie neobsahuje žiadne osobitné pravidlá týkajúce sa nahlasovania, v súlade s jeho odôvodnením 40 žiadne ustanovenie nariadenia nebráni členským štátom a Europolu využívať nahlasovanie ako nástroj na riešenie teroristického obsahu online.

Jednotka EÚ pre nahlasovanie internetového obsahu v Europole od zriadenia v roku 2015 aktívne identifikuje teroristický obsah online a nahlasuje ho poskytovateľom hostingových služieb, ako aj vytvára nástroje (t. j. PERCI a predtým IRMA[16]) na uľahčenie nahlasovania.

Podľa informácií poskytnutých Komisii orgány členských štátov naďalej využívajú nahlasovanie pri určitých poskytovateľoch hostingových služieb, zatiaľ čo prípadne zvažujú vydanie príkazov na odstránenie poskytovateľom hostingových služieb, ktorí nereagujú na nahlasovanie, alebo z iných dôvodov, napríklad naliehavej potreby odstrániť obsah.

4.8. PODPORA MENŠÍCH POSKYTOVATEĽOV HOSTINGOVÝCH SLUŽIEB PRI VYKONÁVANÍ NARIADENIA

Nariadenie obsahuje rozličné povinnosti poskytovateľov hostingových služieb. Zatiaľ čo veľkí poskytovatelia hostingových služieb majú zvyčajne technické spôsobilosti, ľudské zdroje na

[15] Podrobnejšie: – články 3 a 4: zasielanie príkazov na odstránenie, – článok 3 ods. 6 až 8: spätná väzba poskytovateľov hostingových služieb, – článok 4 ods. 3 až 7: mechanizmus kontroly, – článok 7: podávanie správ, – článok 14 ods. 1: predchádzanie konfliktu záujmov, koordinácia, predchádzanie duplicite, – článok 14 ods. 3: zabezpečený komunikačný kanál, – článok 14 ods. 4: používanie špecializovaného nástroja vytvoreného Europolom, – článok 14 ods. 5: oznámenie bezprostredného ohrozenia života, – odôvodnenie 40: nahlasovanie.

[16] Europol v roku 2016 vyvinul aplikáciu na riadenie nahlasovania internetového obsahu (IRMA) v roku 2016 na podporu nahlasovania (označovania) nezákonného obsahu poskytovateľom online služieb. Najprv bol prístup k aplikácii IRMA udelený zamestnancom Europolu a špecializovaným jednotkám (IRU) v siedmich členských štátoch. Aplikáciu IRMA nahradil systém PERCI 3. júla 2023.

overovanie a znalosti potrebné na vykonávanie nariadenia, malí poskytovatelia môžu mať na tento účel obmedzenejšie finančné, technické a ľudské zdroje a odborné znalosti. Zároveň sa na menších poskytovateľov hostingových služieb čoraz častejšie zameriavajú aktéri s nekalými úmyslami, ktorí chcú zneužiť ich služby. Dôvodom môže byť aj účinné úsilie väčších poskytovateľov hostingových služieb o moderovanie obsahu. Hoci tento trend poukazuje na úspech opatrení na moderovanie obsahu, zdôrazňuje sa ním aj potreba podporovať menších poskytovateľov hostingových služieb pri zvyšovaní ich kapacity a znalostí potrebných na dosiahnutie súladu s požiadavkami nariadenia.

S cieľom reagovať na tento problém Komisia uverejnila výzvu na predkladanie návrhov v rámci Fondu pre vnútornú bezpečnosť na podporu menších poskytovateľov hostingových služieb pri vykonávaní nariadenia[17]. Komisia vybrala tri projekty[18] na ich podporu trojitým prístupom. Po prvé tým, že bude informovať a zvyšovať povedomie o pravidlách a požiadavkách nariadenia, po druhé tým, že vyvinie, zavedie a bude vykonávať nástroje a rámce potrebné na riešenie šírenia teroristického obsahu online, a po tretie výmenou skúseností a najlepších postupov v rámci celého odvetvia.

Tieto tri projekty sa začali realizovať v roku 2023 a už priniesli cenné výsledky. Napríklad v mapovacej správe v rámci projektu FRISCO[19] sa zistilo, že mikro a malí poskytovatelia hostingových služieb zvyknú mať obmedzené množstvo informácií a znalostí o nariadení, a zdôraznili sa potenciálne ťažkosti, ktorým by mohli čeliť pri reakcii na príkazy na odstránenie do jednej hodiny, keďže často neponúkajú nepretržité služby 24 hodín denne a 7 dní v týždni. Výzvu predstavuje nedostatok zdrojov, ako aj zriaďovanie komunikačných kanálov s orgánmi presadzovania práva. Vyše polovica poskytovateľov hostingových služieb, ktorých sa dopytovali dodávatelia, nemoderuje obsah vytvorený používateľmi, pričom uviedli, že na svojich platformách sa nikdy nestretli s teroristickým obsahom. U týchto poskytovateľov hostingových služieb je pravdepodobné, že prijmú *ad hoc* opatrenia, ak by sa takýto obsah objavil na ich platforme.

Vďaka týmto trom projektom sa malým poskytovateľom hostingových služieb poskytuje podpora pri ich úsilí o splnenie pravidiel nariadenia aj tým, že sa zriaďujú kontaktné miesta a zavádzajú mechanizmy pre sťažnosti používateľov.

Okrem toho najmä pre menších poskytovateľov hostingových služieb môže byť relevantný článok 3 ods. 2 nariadenia, v ktorom sa vyžaduje včasné poskytovanie informácií o uplatniteľných

[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.

[18] 1. Rámec založený na umelej inteligencii na podporu mikro (a malých) poskytovateľov hostingových služieb pri nahlasovaní a odstraňovaní teroristického obsahu online (ALLIES); 2. Fighting terrorist Content Online (FRISCO – Boj proti teroristickému obsahu online) a 3. Technology Against Terrorism Europe (TATE – Boj proti terorizmu v Európe pomocou technológií). Financovanie a ponuky (europa.eu).

[19] Uskutočnila sa v priebehu šiestich mesiacov do mája 2023. Správa vychádza zo spätnej väzby 48 európskych poskytovateľov hostingových služieb, 33 odpovedí prostredníctvom nášho online prieskumu a 15 odpovedí prostredníctvom rozhovorov. FRISCO, *D2.1: Mapping Report on needs and barriers for compliance Understanding small and micro hosting service providers' needs and awareness in relation to implementing the TCO Regulation requirements* (Mapovacia správa o potrebách a prekážkach v súvislosti s dosiahnutím súladu – Porozumenie potrebám malých a mikroposkytovateľov hostingových služieb a ich informovanosť o požiadavkách nariadenia o teroristickom obsahu online), k dispozícii na adrese: Výsledky | Frisco (friscoproject.eu).

postupoch a lehotách poskytovateľom hostingových služieb, ktorým predtým nebol vydaný príkaz na odstránenie.

4.9. ZÁRUKY TÝKAJÚCE SA ZÁKLADNÝCH PRÁV

Nariadenie obsahuje rôzne záruky na posilnenie zodpovednosti a transparentnosti, pokiaľ ide o opatrenia prijaté na odstránenie teroristického obsahu online. V tejto súvislosti sa odkazuje na uvedené skutočnosti, najmä na informácie poskytnuté o prostriedkoch nápravy, podávaní správ a osobitnom mechanizme pre cezhraničné príkazy na odstránenie.

Okrem toho v článku 23 nariadenia sa vyžaduje, aby Komisia podala správu o fungovaní a účinnosti mechanizmov záruk, najmä tých, ktoré sú stanovené v článku 4 ods. 4, článku 6 ods. 3 a článkoch 7 až 11, v kontexte hodnotenia nariadenia. Takéto záruky sa týkajú sťažností, prostriedkov nápravy a prijatých a vykonávaných mechanizmov sankcií, aby sa predišlo riziku chybného odstránenia teroristického obsahu online v snahe chrániť poskytovateľov obsahu a poskytovateľov hostingových služieb. Posúdenie fungovania a účinnosti mechanizmov záruk bude preto súčasťou hodnotenia podľa článku 23.

V tejto súvislosti sa v programe monitorovania uvedenom v článku 21 ods. 2 nariadenia stanovuje rámec ukazovateľov na hodnotenie vplyvu nariadenia na základné práva, čo bude podkladom pre hodnotenie nariadenia.

Program monitorovania bude podporou pre posúdenie fungovania a účinnosti mechanizmov záruk vykonávaných v kontexte nariadenia a ich vplyvu na základné práva, ktoré sa má vykonať v rámci hodnotenia. V tejto oblasti vplyvu sa zohľadňujú dve oblasti uvedené v článku 23 nariadenia: a) fungovanie a účinnosť mechanizmov záruk, najmä tých, ktoré sú stanovené v článku 4 ods. 4, článku 6 ods. 3 a článkoch 7 až 11, a b) vplyv uplatňovania tohto nariadenia na základné práva, najmä na slobodu prejavu a právo na informácie, rešpektovanie súkromného života a ochranu osobných údajov.

4.10. PRÍSLUŠNÉ ORGÁNY (článok 13)

Podľa článku 13 nariadenia členské štáty musia zabezpečiť, aby ich príslušné orgány mali potrebné právomoci a dostatočné zdroje na dosiahnutie cieľov a plnenie svojich povinností podľa nariadenia. Niektoré členské štáty zaviedli nasledujúce opatrenia, aby zabezpečili potrebné právomoci a dostatočné zdroje príslušných orgánov:

- zriadenie nových orgánov/riaditeľstiev,
- pridelenie dodatočného financovania a dodatočných zamestnancov a
- vytvorenie nových legislatívnych rámcov.

5. ZÁVER

Je mimoriadne dôležité, aby sa v plnej miere zaviedli všetky nástroje a opatrenia na úrovni EÚ s cieľom urýchlene riešiť nezákonný obsah šírený online. Má to veľký význam najmä vzhľadom

na obrovský rozsah takéhoto nezákonného obsahu, ktorý sa objavuje v poslednom období, keď sa šíri obsah týkajúci sa útoku, ktorý spáchal Hamas proti Izraelu.

Nariadenie prispieva k zvyšovaniu verejnej bezpečnosti v celej Únii s cieľom zabrániť tomu, aby teroristi využívali poskytovateľov hostingových služieb pôsobiacich na vnútornom trhu na šírenie svojich odkazov, ktorými zastrašujú, radikalizujú, uskutočňujú nábor a uľahčujú teroristické útoky.

V nadväznosti na začatie konaní o nesplnení povinnosti v januári 2023 **sa dosiahol pokrok**. K 31. decembru 2023 určilo 23 členských štátov príslušné orgány podľa článku 12 ods. 1, ako sa uvádza v online registri, čo viedlo k systematickejšiemu využívaniu opatrení a nástrojov stanovených v nariadení. Navyše 11 z 22 prípadov nesplnenia povinnosti začatých v januári 2023 bolo do 21. decembra 2023 uzavretých. Komisia naliehavo vyzýva ostatné členské štáty, aby prijali potrebné opatrenia na určenie príslušných orgánov podľa článku 12 ods. 1 a splnili si povinnosti podľa článku 12 ods. 2 a 3 a článku 18 ods. 1.

Členské štáty vo všeobecnosti oznámili bezproblémové zasielanie príkazov na odstránenie poskytovateľom hostingových služieb s podporou Europolu. Na základe informácií získaných od členských štátov a Europolu sa od nadobudnutia účinnosti nariadenia zaslalo najmenej 349 **príkazov na odstránenie teroristického obsahu**. V desiatich prípadoch jeden poskytovateľ hostingových služieb teroristický obsah neodstránil/nezablokoval prístup k nemu do jednej hodiny, čo je maximálna lehota stanovená v nariadení.

Podľa informácií získaných od členských štátov a Europolu sa napriek tomu, že nariadenie v tomto ohľade nezahŕňa žiadne pravidlá, od nadobudnutia účinnosti nariadenia zvýšila schopnosť reagovať na nahlasovanie teroristického obsahu. Okrem toho Europol dostal od poskytovateľov hostingových služieb informácie o deviatich prípadoch výskytu teroristického obsahu, ktorý zahŕňa bezprostredné ohrozenie života, ako sa uvádza v článku 14 ods. 5.

Efektívnejšie komunikačné kanály a postupy fungujú najmä od uvedenia platformy PERCI do prevádzky 3. júla 2023, čo viedlo k systematickejšiemu prístupu k zasielaniu príkazov na odstránenie, pričom platforma PERCI sa často využíva aj na nahlasovanie. Členské štáty a Europol vyjadrili očakávanie, že uvedenie platformy PERCI do prevádzky pomôže využívať tieto nástroje na boj proti teroristickému obsahu online.

Na základe uvedených skutočností Komisia dospela k záveru, že nariadenie celkovo malo **pozitívny vplyv** na obmedzenie šírenia teroristického obsahu online. Napriek tomu v desiatich prípadoch zo 349 dotknutý poskytovateľ hostingových služieb pri odstraňovaní teroristického obsahu alebo zablokovaní prístupu k nemu prekročil maximálnu lehotu jednej hodiny stanovenú v nariadení.

Komisia aktívne podporuje členské štáty a poskytovateľov hostingových služieb, a to aj technickými workshopmi, ktoré zorganizovala pred nadobudnutím účinnosti nariadenia aj po ňom. Posledný workshop sa uskutočnil 24. novembra 2023. Komisia takisto podporuje menších poskytovateľov hostingových služieb s cieľom zabezpečiť úplné a rýchle uplatňovanie nariadenia a pomáha im pri riešení výziev, ktoré sa doteraz vyskytli.

Komisia bude vykonávanie a uplatňovanie tohto nariadenia naďalej monitorovať. Komisia bude dôkladne monitorovať výkonnosť nástrojov stanovených v nariadení prostredníctvom programu monitorovania, ktorý bude podkladom pre hodnotenie nariadenia podľa článku 23.