tech against terrorism europe

Zefektívnenie postupov na boj proti terorizmu

Sprievodca šiestimi krokmi na dodržiavanie nariadenia EÚ o TCO

Sophia Rothut, Heidi Schulze, Diana Rieger, Catherine Bouko & Brigitte Naderer

Preklad od Jakub Rybár (CMS)

DCU GHENT UNIVERSITY jos LMU SAHER EUROPE Swansea University Prifysgol Abertawe tech against terrorism

Funded by the European Union

Tech Against Terrorism Europe (TATE)

Táto príručka je súčasťou projektu Tech Against Terrorism Europe (TATE). Projekt TATE financuje Európska únia (ISF-2021-AG-TCO-101080101). Tento projekt podporuje menších poskytovateľov hostingových služieb pri budovaní ich protiteroristických štruktúr a pri podávaní správ o transparentnosti, ako sa vyžaduje v nariadení EÚ o riešení šírenia teroristického obsahu online (nariadenie o TCO) a v smernici (EÚ) 2017/541.

tate.techagainstterrorism.org

Funded by the European Union

Autorky

Sophia Rothut je výskumnou pracovníčkou v laboratóriu profesorky Riegerovej (LMU Mníchov). V rámci európskeho projektu TATE sa zaoberá požiadavkami na boj proti teroristickému obsahu na internete. Jej výskum sa zameriava na online radikalizáciu, presadzovanie radikálnych myšlienok a politických/krajne pravicových influencerov.

Heidi Schulze je výskumnou pracovníčkou na Katedre médií a komunikácie na LMU v Mníchove. Na LMU je súčasťou výskumného laboratória profesorky Riegerovej a skúma dynamiku online radikalizácie v rámci rozsiahleho výskumného projektu MOTRA - Radicalization Monitoring System and Transfer Platform. Vo svojom výskume sa zameriava na radikalizačnú/extrémistickú (skupinovú) komunikáciu na alternatívnych sociálnych platformách a v okrajových komunitách, ako aj na charakteristiky a publikum hyper-partizánskych spravodajských webových stránok.

Diana Rieger je profesorkou na Katedre médií a komunikácie na LMU v Mníchove. Venuje sa výskumu online radikalizácie, nenávistných prejavov a účinkov obsahu určeného pre zábavu. Publikovala tiež na tému vývoja a hodnotenia protiopatrení na boj proti radikalizácii.

Catherine Bouko je docentkou komunikácie a francúzštiny na Univerzite v Gente (Belgicko). Jej hlavným predmetom výskumu je politická komunikácia, extrémizmus a občianstvo na sociálnych sieťach, pričom sa zameriava najmä na komunikáciu založenú na obrazoch. Metodologicky využíva (multimodálnu) analýzu diskurzu, kvantitatívnu obsahovú analýzu, semiotiku a etnografiu.

Brigitte Naderer je post doktorandkou v Centre pre verejné zdravie (Center for Public Health), oddelenie sociálnej a preventívnej medicíny, odbor výskumu samovrážd a podpory duševného zdravia na Lekárskej univerzite vo Viedni. Predtým pôsobila na Katedre médií a komunikácie LMU v Mníchove, kde pracovala do marca 2023. Jej výskum sa zameriava na mediálnu gramotnosť, online radikalizáciu a vplyv médií na deti a dospievajúcich.

Poďakovanie: Ďakujeme organizácii Tech Against Terrorism za ich príspevky a pripomienky k tejto príručke. Taktiež by sme chceli poďakovať profesorke Maure Conwayovej za jej užitočné postrehy.

Táto verzia bola do slovenčiny preložená Analytickým odborom Rady pre mediálne služby.

Obsah

A. Úvod

O čom je táto príručka a prečo by ste si ju mali prečítať...

Táto príručka sa zaoberá **povinnosťami, ktoré poskytovateľom hostingových služieb (z angl. „hosting service providers", ďalej iba HSP) ukladá** Európske nariadenie o šírení teroristického obsahu online (nariadenie o TCO) prijaté v apríli 2021. Zaoberá sa tým, čo musia HSP zohľadniť v boji proti šíreniu teroristického obsahu online a poskytuje praktické rady, ako na tento účel zaviesť rôzne opatrenia.

Príručka sa zameriava predovšetkým na **minimálne požiadavky, ktoré musia HSP spĺňať, aby boli v súlade s nariadením o TCO**. Ďalej poskytuje **tipy a praktické rady týkajúce sa príslušných (pro)aktívnych opatrení, ktoré by HSP mali prijať**, aby sa úspešne orientovali v zložitosti regulačného postupu presadzovania (t. j. čo robiť, keď sa vo vašej poštovej schránke objaví príkaz na odstránenie) a aby sa HSP pripravili na boj proti teroristickému zneužívaniu svojich platforiem.

Príručka je súčasťou projektu Tech Against Terrorism Europe (TATE), ktorý financuje Európska komisia. Konzorcium TATE tvorí sedem partnerov: Dublin City University, Ghent University, JOS Project, LMU Munich, Saher Europe, Swansea University a Tech Against Terrorism. Cieľom projektu TATE je vytvoriť povedomie o európskom nariadení o TCO a podporiť malé technologické spoločnosti a mikropodniky, aby prijali opatrenia na jeho podporu. Spolu s ďalšími zdrojmi vytvorila TATE túto príručku s cieľom čo najviac priblížiť HSP právne a praktické očakávania.

Komu je táto príručka určená?

Príručka je určená HSP a ich zamestnancom, ako aj IT odborníkom, ktorí chcú implementovať technické prvky na boj proti teroristickému obsahu do štruktúr platforiem. Jej cieľom je poskytnúť informácie o minimálnych požiadavkách, ktoré musia byť splnené, aby sa dosiahol súlad s európskym nariadením o TCO.

Túto príručku a ďalšie zdroje TATE sme vytvorili na podporu malých a mikroposkytovateľov HSP. Uvedomujeme si, že malí a mikro HSP majú často obmedzené zdroje na riešenie teroristického obsahu na svojich platformách. **Je však veľmi dôležité, aby malí a mikro HSP nezanedbávali túto hrozbu, pretože pri menších platformách je väčšia pravdepodobnosť, že ich zneužijú teroristickí aktéri** (podrobnosti nájdete v tejto správe Tech Against Terrorism).

Aké sú základné prvky európskeho nariadenia o riešení šírenia teroristického obsahu online (TCO)?

Európske nariadenie o riešení šírenia teroristického obsahu online (TCO) vstúpilo do platnosti v júni 2022 a **ukladá HSP povinnosť odstrániť obsah alebo znemožniť k nemu prístup do jednej hodiny od prijatia príkazu na odstránenie od príslušného orgánu**.

HSP musia spolupracovať s orgánmi presadzovania práva, ako je napríklad Europol, a tiež s inými príslušnými orgánmi pri odhaľovaní a odstraňovaní teroristického obsahu, ktorý sa môže nachádzať na ich platformách. Na dosiahnutie súladu s nariadením o TCO **musia HSP implementovať aj účinné a primerané opatrenia na zabránenie opätovného nahrávania teroristického obsahu** a musia dodržiavať ďalšie povinnosti, o ktorých sa dozviete v tejto príručke.

Ako je táto príručka štruktúrovaná?

Nariadenie o TCO v súčasnosti vyžaduje, aby HSP:

1) Vypracovali príslušné podmienky poskytovania služieb (▶kapitola 1),
2) Prijali osobitné opatrenia na identifikáciu a odstránenie teroristického obsahu (▶kapitola 2),
3) Zriadili účinné mechanizmy moderovania (▶kapitola 3),
4) Zriadili kontaktné miesta a právnych zástupcov (▶kapitola 4),
5) Vytvorili mechanizmy nahlasovania užívateľom a podávania sťažností (▶kapitola 5),
6) Zverejňovali správy o transparentnosti (▶kapitola 6).

Vysvetlenia a odporúčania uvedené v tejto príručke sme štrukturovali podľa týchto šiestich hlavných požiadaviek. Na začiatku každej kapitoly nájdete krátke zhrnutie obsahu kapitoly a jej hlavných bodov. Následne vám poskytneme podrobné informácie o tom, čo nariadenie o TCO vyžaduje alebo vyzýva HSP aby zaviedli, ako aj ďalšie praktické rady na ochranu vašej platformy pred teroristickým (a iným škodlivým) obsahom.

Ktorých platforiem sa týka nariadenie o TCO?

Nariadenie o TCO sa týka HSP, čo zahŕňa všetky platformy, ktoré umožňujú používateľom šíriť informácie smerom k verejnosti prostredníctvom svojich služieb.

Nariadenie o TCO sa vzťahuje na **poskytovateľov hostingových služieb (HSP) všetkých veľkostí a na každého HSP, ktorý ponúka svoje služby v EÚ**. Vzťahuje sa aj na HSP so sídlom mimo EÚ, ak HSP (1) má významný počet používateľov v jednom alebo viacerých členských štátoch EÚ alebo (2) zameriava svoje činnosti na jeden alebo viacero členských štátov EÚ.

Kedy sa HSP považuje za "vystaveného teroristickému obsahu"?

Nariadenie o TCO ukladá osobitné opatrenia HSP, ktorí sú "vystavení teroristickému obsahu". Podľa čl. 5 ods. 4 k takémuto vystaveniu dochádza vtedy, ak HSP boli oznámené a prijaté dva alebo viac konečných príkazov na odstránenie v predchádzajúcich 12 mesiacoch od príslušného orgánu členského štátu, v ktorom má HSP svoje hlavné miesto podnikateľskej činnosti alebo svojho právneho zástupcu v EÚ.

Čo je teroristický obsah?

Keďže nariadenie o TCO sa týka teroristického obsahu šíreného online, je kľúčové poskytnúť jeho definíciu. Smernica EÚ 2017/541 stanovuje základ pre nariadenie o TCO tým, že definuje, čo sa rozumie pod teroristickým obsahom.

Obsah sa považuje za teroristický, ak podnecuje na spáchanie činov alebo podporuje úmysly v prospech teroristických zámerov, čím priamo alebo nepriamo prispieva k hrozbe teroristických trestných činov.

Za teroristický obsah sa považuje aj vyhrážanie sa spáchaním teroristického trestného činu, ako aj poskytovanie informácií, podpory alebo financovania týchto činov.

Druhy trestných činov terorizmu

Trestné činy terorizmu môžu zahŕňať (smernica EÚ 2017/541, Art. 3.1):

- Útoky na život alebo fyzickú integritu osoby.
- Únos alebo branie rukojemníka.
- Spôsobenie rozsiahleho poškodenia špecifických zariadení a infraštruktúry (napr. vládnych/verejných zariadení, dopravných a informačných systémov), ktoré môže ohroziť ľudský život alebo mať za následok vážnu hospodársku stratu.
- Ovládnutie lietadiel, lodí alebo iných prostriedkov verejnej alebo nákladnej dopravy.
- Výroba, držanie, získanie, preprava, dodávka alebo použitie výbušnín alebo zbraní, vrátane chemických, biologických, rádiologických alebo jadrových zbraní, ako aj výskum a vývoj chemických, biologických, rádiologických alebo jadrových zbraní.
- Uvoľnenie nebezpečných látok alebo spôsobenie požiaru, záplav alebo výbuchov a narušenie základných zdrojov (napr. vody, energie), ktorých následkom je ohrozenie ľudského života.
- Zasahovanie do dodávok vody, energie alebo iných základných prírodných zdrojov alebo ich prerušenie, ktorých následkom je ohrozenie ľudského života.

Za trestný čin sa považuje aj riadenie teroristickej skupiny alebo úmyselná účasť na jej činnosti (smernica EÚ 2017/541, článok 4). Patrí sem aj poskytovanie (informačných) zdrojov (napr. návodov alebo materiálov na výrobu zbraní) na teroristické účely alebo financovanie takýchto aktivít.

Cieľom teroristických činov je a) vážne zastrašiť obyvateľstvo, b) neoprávnene donútiť vládu alebo medzinárodnú organizáciu k určitému konaniu alebo zdržaniu sa konania, alebo c) vážne destabilizovať alebo zničiť základné politické, ústavné, hospodárske alebo sociálne štruktúry krajiny alebo medzinárodnej organizácie (smernica EÚ 2017/541, článok 3 ods. 2) .

Stručne povedané, obsah sa považuje za teroristický, ak umožňuje, podporuje alebo uľahčuje spáchanie teroristického trestného činu alebo ak obsahuje hrozbu spáchania teroristického trestného činu.

B. Kľúčové povinnosti a odporúčania v súvislosti s nariadením o TCO

V nasledujúcich kapitolách nájdete informácie o šiestich kľúčových zložkách nariadenia o TCO a o krokoch na zabezpečenie vašej platformy proti hrozbe terorizmu. Patria medzi ne nasledujúce kľúčové oblasti a otázky.

Kapitola 1: Vypracovanie a uplatňovanie podmienok služby zakazujúcich teroristický obsah

1. Čo sú to podmienky poskytovania služieb (ToS)?
2. Prečo je potrebné mať jasné a robustné ToS?
3. Praktické tipy a rady: Aké sú prvky spoľahlivých ToS?

Kapitola 2: Osobitné opatrenia na identifikáciu a odstránenie (teroristického) obsahu

1. Prečo je potrebné zaviesť procesy identifikácie nezákonného a škodlivého obsahu?
2. Proces identifikácie teroristického obsahu
3. Praktické tipy a rady: Čo pomáha posúdiť, či je obsah nezákonný?
4. Čo mám robiť, ak to vidím inak? Ako namietať proti prijatému príkazu na odstránenie

Kapitola 3: Zavedenie účinných mechanizmov moderovania teroristického obsahu online

1. Čo je moderovanie obsahu a prečo je v niektorých prípadoch potrebné?
2. Praktické tipy a rady: Ako by sa mala moderácia obsahu vykonávať?
3. Alternatívne prístupy k moderovaniu

Kapitola 4: Zriadenie kontaktných miest a právnych zástupcov

1. Čo sú to kontaktné miesta a právni zástupcovia?
2. Prečo je potrebné mať kontaktné miesto alebo právneho zástupcu?
3. Čo je to príslušný orgán členského štátu EÚ a ako ho kontaktovať?

Kapitola 5: Nastavenie systému nahlasovania užívateľmi a podávania sťažností na odstránený obsah

1. Prečo je potrebné zriadiť transparentný mechanizmus podávania sťažností?
2. Aké sú požiadavky na systém podávania sťažností?
3. Ako sa majú sťažnosti vybavovať a aké sú možné výsledky?
4. Praktické tipy a rady: Aké prvky sú užitočné pri vytváraní systému sťažností?

Kapitola 6: Praktická podpora a poradenstvo v oblasti správ o transparentnosti

1. Čo sú správy o transparentnosti?
2. Prečo sú správy o transparentnosti potrebné?
3. Postup prípravy správ o transparentnosti.
4. Aké informácie a metriky musia byť zahrnuté v správe o transparentnosti TCO?

V príručke sa vysvetľujú **aspekty nariadenia o TCO, ktoré sú pre platformy najdôležitejšie, a zároveň sa v nej poskytujú praktické rady týkajúce sa proaktívnych opatrení, ktoré možno prijať na boj proti šíreniu škodlivého obsahu online**. Takéto opatrenia sú nevyhnutné na prípravu platforiem proti zneužívaniu ich služieb teroristami - alebo povedané jazykom nariadenia o TCO: aby ste boli schopní zvládnuť situáciu, keď vám v poštovej schránke pristane prvý a každý ďalší príkaz na odstránenie.

Kapitola 1

Vypracovanie a uplatňovanie podmienok služby zakazujúcich teroristický obsah

Zhrnutie: Obsah a hlavné body tejto kapitoly

- Podmienky používania služby (ToS) sú **záväznou dohodou** medzi používateľom a HSP, ktorá definuje vhodné a povolené používanie platformy.
- HSP musia (1) vo svojich ToS stanoviť svoju **stratégiu riešenia šírenia teroristického obsahu** a (2) **zakázať** šírenie **teroristického obsahu**.
- Okrem toho a nad rámec nariadenia o TCO môžu a mali by HSP zvážiť zákaz iných foriem škodlivého obsahu (napr. extrémistického obsahu, nenávistných prejavov).
- ToS sú **právnou nevyhnutnosťou** podľa nariadenia o TCO a môžu tiež zakomponovať **užitočnú ochranu platformy**.
- Na to, aby boli vaše ToS čo najspoľahlivejšie, sa vyžaduje niekoľko prvkov vrátane definovania teroristického obsahu a zverejnenia stratégie HSP na boj proti teroristickému obsahu na danej platforme.

Vhodné podmienky **poskytovania služieb (z angl. Terms of Service, ďalej iba „ToS“) sú základom pre zákaz a následné spracovanie teroristického obsahu**. Nariadenie o TCO výslovne vyzýva HSP, aby stanovili “svoju politiku riešenia šírenia teroristického obsahu vrátane prípadného relevantného vysvetlenia fungovania osobitných opatrení, čo v relevantných prípadoch zahŕňa aj používanie automatizovaných nástrojov” (nariadenie o TCO, článok 7 ods.1).

Okrem toho a nad rámec nariadenia o TCO môžu a mali by HSP **zvážiť zákaz iných foriem škodlivého obsahu** (napr. extrémistického obsahu, nenávistných prejavov, propagácie násilia) vo svojich ToS. Týmto spôsobom môžu HSP prispieť k vytvoreniu rámca pre občiansku digitálnu kultúru.

1. Čo sú to podmienky poskytovania služieb (ToS)?

ToS sú pravidlá stanovené konkrétnymi platformami a pre konkrétne platformy, ktoré definujú (1) povinnosti HSP voči ich používateľom a (2) vhodné a povolené, ale aj zakázané správanie a obsah na danej platforme. Používatelia musia tieto podmienky prijať, ak chcú využívať služby HSP.

Synonymá používané pre ToS sú napríklad podmienky používania, podmienky a ustanovenia alebo komunitné štandardy. Nariadenie o TCO používa výraz "podmienky" a definuje ho ako "všetky podmienky a ustanovenia bez ohľadu na ich názov alebo formu, ktorými sa riadi zmluvný vzťah medzi HSP a jeho používateľmi" (nariadenie o TCO, článok 2.8).

2. Prečo je potrebné mať jasné a robustné ToS?

Pre hlbší pohľad na to, prečo je potrebné mať jasné a robustné ToS, predstavíme dva rôzne pohľady: právny a podnikový/prevádzkový.

a) Právne hľadisko

Súlad s (EÚ) právnymi predpismi

ToS musia byť v súlade s platnými právnymi predpismi (EÚ) vrátane nariadenia o TCO, ale aj smernice EÚ 2017/541, ktorá posilňuje riešenie teroristického obsahu v celej EÚ tým, že (1) definuje teroristický obsah, (2) stanovuje zaň sankcie (článok 15), (3) posilňuje práva obetí a ich podporu a (4) uznáva terorizmus ako nadnárodnú, cezhraničnú hrozbu. Nariadenie o TCO aj uvedená smernica podporujú celoeurópsku a medzinárodnú spoluprácu. ToS sú miestom, kde môžu HSP zdôrazniť svoj záväzok bojovať proti teroristickými aktivitám.

Ochrana HSP pred právnou zodpovednosťou

ToS sú určené na ochranu HSP pred zodpovednosťou (pokiaľ sú ToS v súlade s platnými právnymi predpismi). Keďže ide o zmluvu medzi HSP a jeho používateľmi, ToS sú právne záväznou dohodou medzi týmito dvoma stranami. ToS umožňujú HSP stanoviť pravidlá (ne)prijateľného používania v súlade s hodnotami HSP.

Odôvodnenie (proaktívneho) odstraňovania obsahu

Jasné ToS sú dôležité pri stretávaní sa s problematickým obsahom a jeho moderovaní. HSP sa môžu pri zdôvodňovaní moderovania obsahu odvolávať na svoje ToS, ak obsahujú podrobné informácie o zakázaných praktikách týkajúcich sa obsahu vrátane zákazu terorizmu.

b) Hľadisko spoločnosti

Údržba prevádzkovej činnosti

V prvom rade je dodržiavanie právnych predpisov kľúčové pre prevádzkovú činnosť HSP, a teda aj pre úspech spoločnosti. HSP majú určitú zodpovednosť voči svojim akcionárom, ktorí dodržiavanie právnych predpisov očakávajú. Okrem toho môže vzniknúť finančná zodpovednosť a ďalšími možnými dôsledkami nedodržiavania sú regulačné sankcie alebo poškodenie dobrého mena.

Prejavenie občianskej zodpovednosti HSP

V druhom rade, ako významné spoločenské subjekty majú HSP zodpovednosť voči verejnosti, a to kolektívnu aj individuálnu. Zodpovednosť voči verejnosti vo všeobecnosti zahŕňa boj proti nezákonným činnostiam, ako je terorizmus a odhaľovanie či predchádzanie teroristickému obsahu predtým, ako sa začne vo veľkom šíriť. Tým, že HSP v ToS uvedú, že nezákonné činnosti sú zakázané, položia základ bezpečnejšej online sféry a môžu sa naň spoľahnúť pri zásahoch proti nezákonnému obsahu. Jednoznačné ToS tiež pomáhajú spoločnostiam preukázať svoju zodpovednosť voči jednotlivým členom verejnosti budovaním dôvery

prostredníctvom transparentnosti. V tomto ohľade HSP demonštrujú jednotlivým používateľom, že budú chránení pred škodlivým obsahom na platforme, keď je takýto obsah v ich ToS výslovne a vynútiteľne zakázaný.

3. Praktické tipy a rady: Aké sú prvky spoľahlivých ToS?

Nasledujúce časti obsahujú usmernenia týkajúce sa prvkov, ktoré by ste ako HSP mali zvážiť pri vypracúvaní ToS v kontexte nariadenia o TCO.

Je dôležité zdôrazniť, že tvorba ToS je iteračný proces: ToS sa môžu a mali by sa v prípade potreby upravovať, napríklad v reakcii na návrhy používateľov a v súlade s vývojom vnútroštátnych alebo medzinárodných právnych predpisov. V nariadení o TCO sa vyžaduje takáto prispôsobivosť: HSP, ak sú vystavení teroristickému obsahu, sú povinní zmeniť svoje ToS tak, aby to uviedli a **stanovili, aké opatrenia budú prijaté na boj proti zneužívaniu platformy na teroristické účely** (nariadenie o TCO, článok 5 ods. 1).

Konkrétne odporúčame venovať pozornosť **jasnosti a štruktúre** ToS. Zo štúdií vyplýva, že používatelia trávia málo času čítaním ToS a nevenujú dostatočnú pozornosť prezentovaným informáciám; ToS skôr pôsobia ako usmerňovač všeobecného vnímania používateľov o tom, čo je povolené a čo nie[1,2]. Na uľahčenie navigácie a pochopenia ToS sa odporúča investovať čas do vizuálneho návrhu ToS a pracovať s jasnými nadpismi alebo bodovými zoznamami. Môže byť tiež užitočné z času na čas pripomenúť používateľom aspekty ToS a v prípade zistenia podozrivého správania upozorniť na možné dôsledky (napr. prostredníctvom vyskakovacieho okna)[2].

Pri nastavovaní a revízii ToS **môže** nasledujúci **kontrolný zoznam slúžiť ako návod na optimalizáciu súladu s nariadením o TCO.**

Definovanie teroristického obsahu

Existencia funkčných definícií terorizmu a teroristického obsahu je dôležitá pre opatrenia proti takémuto obsahu a správaniu. Tieto definície by mali byť uvedené v ToS a malo by sa na ne odkazovať pri vyhodnocovaní obsahu. Existujúce definície, ktoré už boli predstavené a diskutované v tejto príručke (► viď definíciu tu), najmä definície EÚ založené na smernici EÚ 2017/541, môžu v tomto ohľade poskytnúť užitočné usmernenie.

Zverejnenie stratégie boja proti teroristickému obsahu

Nariadenie o TCO ukladá HSP, ktorí sú vystavení teroristickému obsahu, povinnosť vysvetliť vo svojich ToS stratégiu boja proti šíreniu takéhoto obsahu, ako aj všetky používané automatizované prostriedky (napr. pri identifikácii zakázaného obsahu; ► kapitola 2). Nariadenie o TCO ďalej vyžaduje, aby HSP po vystavení teroristickému obsahu zaviedli osobitné opatrenia (napr. systémy na nahlasovanie škodlivého obsahu od používateľov,

[1] Obar, J. A., & Oeldorf-Hirsch, A. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society*, *23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870
[2] Robinson, E. P., & Zhu, Y. (2020). Beyond "I Agree": Users' Understanding of Web Site Terms of Service. *Social Media + Society*, *6*(1), 1–13. https://doi.org/10.1177/2056305119897321

systémy na podávanie sťažností na odstránenie obsahu; ► kapitola 4) (nariadenie o TCO, čl. 7.1).

Používanie označovacích zoznamov a zváženie jasného zákazu iných kategórií škodlivých foriem obsahu

Rôzne typy obsahu môžu byť škodlivé pre používateľov, spoločnosť a samotnú platformu. HSP by preto mali zvážiť nasledujúce dodatočné zákazy, ktoré sú upravené aj v iných právnych rámcoch, ako je nariadenie o digitálnych službách (DSA), a teda zakázať obsah obsahujúci napríklad nenávistné prejavy alebo podnecovanie k násiliu. Na úrovni aktérov môžu byť z používania platformy vylúčené teroristické skupiny. Dobrým zdrojom takýchto zákazov sú označovacie zoznamy (t. j. oficiálne zoznamy teroristických skupín zverejnené demokratickými štátmi). Okrem toho môžu príslušné orgány upozorniť HSP na obsah, ktorý nemožno klasifikovať ako teroristický, ale napriek tomu je škodlivý; posúdenie obsahu z hľadiska ToS a prípadné riešenie neteroristického, ale škodlivého obsahu je v konečnom dôsledku zodpovednosťou HSP (nariadenie o TCO, 40).

Komunikácia akceptovaného používania

ToS by tiež mali s odkazom na hodnoty a účel platforiem popisovať, aké spôsoby používania sú nielen akceptované, ale aj vítané a podporované zo strany HSP. Na to neexistuje univerzálny štandard - značne sa líši v závislosti od funkcionalít a princípov platformy. Vzhľadom na to sa opis podporovaného používania výslovne nevyžaduje na splnenie povinností vyplývajúcich z nariadenia o TCO.

Poskytnutie informácií o tom, ako nahlásiť zakázaný obsah

Jedným zo spôsobov, ako odhaliť nezákonný obsah a obsah porušujúci ToS, sú nahlasovacie mechanizmy pre používateľov. HSP by preto mali do svojich ToS zahrnúť časť vysvetľujúcu postupy nahlasovania obsahu podozrivého z porušovania ToS.

Stanovenie dôsledkov porušenia ToS

Aby sa zabezpečilo transparentné riešenie porušenia ToS a zachovala sa zodpovednosť voči verejnosti, HSP by mali vo svojich ToS jasne stanoviť opatrenia, ktoré sa majú byť prijaté voči používateľom a/alebo obsahu v prípade porušenia ToS. Podľa nariadenia o TCO však príkaz na odstránenie od príslušného orgánu musí viesť k odstráneniu obsahu do jednej hodiny od jeho označenia. Príkazy na odstránenie môžu byť vykonané aj zablokovaním obsahu alebo jeho geografickým blokovaním v EÚ.

Uverejňovanie výročných správ o transparentnosti

Pri príprave a revízii ToS by sa HSP mali verejne zaviazať k pravidelnému zverejňovaniu správ o transparentnosti. Praktické tipy a regulačné požiadavky nariadenia o TCO na tvorbu správ o transparentnosti nájdete v ► kapitole 6.

Kapitola 2

Osobitné opatrenia na identifikáciu a odstránenie (teroristického) obsahu

Zhrnutie: Obsah a hlavné body tejto kapitoly

- Schopnosť HSP identifikovať obsah ako teroristický je základom pre implementáciu nariadenia o TCO a ďalších.
- V mnohých prípadoch nie je jednoduché prijať rozhodnutie a môže byť **veľmi kontextuálne a citlivé**.
- **Je potrebné starostlivo zohľadniť základné práva, ako je sloboda prejavu**.
- **Pokiaľ ide o nariadenie o TCO, HSP nemusia posudzovať zákonnosť obsahu, na ktorý upozornil príslušný orgán**. Po vydaní príkazu na odstránenie však **majú HSP aj poskytovatelia obsahu (t. j. používatelia) právo napadnúť ho**.
- Odporúča sa stanoviť postup, ktorý bude dodržiavaný pri identifikácii teroristického obsahu. Takýto proces bude pozostávať z viacerých krokov.
- Pri posudzovaní obsahu sú potrebné rôzne spôsoby praktického posudzovania, ako napríklad používanie označovacích zoznamov alebo databáz symbolov, či metód na vykonanie potrebného vyvažovania.
- Navyše, procesy preskúmania zohrávajú obzvlášť dôležitú úlohu v osobitnom prípade **cezhraničných príkazov na odstránenie**, keď HSP nedostane príkaz na odstránenie od príslušného orgánu, v ktorom má hlavné miesto podnikateľskej činnosti alebo právneho zástupcu. V takýchto prípadoch sa uplatňujú **osobitné postupy**.

Je veľmi dôležité, aby HSP dokázali posúdiť, či je obsah nezákonný alebo teroristický, aby mohli proaktívne odhaľovať teroristický obsah, ako aj právne napadnúť príkazy na odstránenie, ak sa HSP domnievajú, že boli vydané chybne. Správna identifikácia obsahu nezákonného a teroristického je dôležitá na to, aby sa zachoval aj inak legálny a neteroristický obsah online. Takéto rozhodnutia sú často náročné a je **vždy potrebné zvážiť škodu spôsobenú obsahom a škodu spôsobenú porušením základného práva na slobodu prejavu**.

1. Zavádzanie procesov identifikácie nezákonného a škodlivého obsahu

Procesy identifikácie zahŕňajú definovaný súbor krokov, ktoré spoločnosti alebo platformy vykonávajú s cieľom určiť, či obsah porušuje nariadenie o TCO alebo niektoré prvky ToS platforiem. Tieto kroky by mali viesť k metodickému posúdeniu a umožniť prijatie odôvodneného rozhodnutia o nezákonnosti obsahu.

Takéto vyvažujúce rozhodnutia sú **potrebné na**: a) **prijatie proaktívnych opatrení** proti teroristickému a/alebo inak škodlivému obsahu a b) **napadnutie sporných prípadov príkazov na odstránenie,** ktoré

vydal príslušný orgán na základe nariadenia o TCO (viac informácií o procese opravných prostriedkov bude nasledovať v tejto kapitole v ► podkapitole 4).

Proaktívne opatrenia proti teroristickému a inému škodlivému obsahu sa odporúčajú z rôznych dôvodov.

1. Implementáciou takýchto opatrení HSP preukazujú spoľahlivosť a dobrú vôľu voči politickým činiteľom s rozhodovacou právomocou, príslušným orgánom a iným relevantným zainteresovaným stranám.
2. Proaktívne opatrenia budujú dôveru zainteresovaných strán, pretože pozitívne delimitujú právnu zodpovednosť alebo poškodenie dobrého mena, ktoré by mohlo vzniknúť teroristickým zneužitím platforiem.
3. Nedostatočné alebo neprimerané opatrenia proti teroristickému, extrémistickému alebo inak škodlivému obsahu môžu viesť k tomu, že platforma priláka používateľov, ktorí majú v úmysle šíriť práve takýto obsah. Dôsledkom toho by bol zvýšený výskyt zakázaného obsahu, ktorý by si následne vyžadoval väčšie časové investície, úsilie a finančné zdroje zo strany HSP na jeho potlačenie.

2. Proces identifikácie teroristického obsahu

1) Vymedzenie teroristického obsahu

Každá klasifikácia obsahu sa vykonáva na základe definície. Pokiaľ ide o nariadenie o TCO, definícia teroristického obsahu je definícia obsiahnutá v smernici EÚ 2017/541, ako sa uvádza v ► úvode. V nej sa teroristický obsah definuje ako textový, vizuálny alebo zvukový

> "materiál, ktorý niekoho podnecuje alebo navádza na páchanie trestných činov terorizmu alebo poskytnutie pomoci pri páchaní týchto činov, niekoho navádza na účasť na činnostiach teroristickej skupiny, alebo glorifikuje teroristické činnosti, vrátane materiálu, ktorý zobrazuje teroristický útok. Okrem toho by toto vymedzenie malo zahŕňať aj materiál, ktorý poskytuje inštrukcie na výrobu alebo používanie výbušnín, strelných zbraní alebo iných zbraní, alebo škodlivých alebo nebezpečných látok, ako aj chemických, biologických, rádiologických a jadrových látok (CBRN), či iných osobitných metód alebo techník vrátane výberu cieľov na účely spáchania trestných činov terorizmu alebo poskytnutia pomoci pri páchaní takýchto činov." (nariadenie o TCO, 11)

Definícia nezahŕňa "materiál šírený na vzdelávacie, novinárske, umelecké alebo výskumné účely alebo na účely zvyšovania povedomia v záujme boja proti teroristickej činnosti" (nariadenie o TCO, 12), a základné práva, ako je sloboda prejavu, informácií a vedy, ktoré musia byť vždy starostlivo zohľadnené. "Okrem toho by sa vyjadrovanie radikálnych, polemických alebo kontroverzných názorov vo verejnej diskusii o citlivých politických otázkach nemalo považovať za teroristický obsah." (nariadenie o TCO, 12)

2) Podpora pomocou automatizovaných nástrojov

Na počiatočnú identifikáciu potenciálne problematického obsahu môže byť užitočné použiť automatizované nástroje. Automatizácia sa môže použiť napríklad na identifikáciu konkrétnych

kľúčových slov spojených s extrémistickými myšlienkami alebo vizuálnymi prvkami, ako sú logá alebo symboly teroristických organizácií. Existujú aj iniciatívy na automatické odhaľovanie potenciálne teroristického obsahu na rôznych platformách prostredníctvom odkazu na spoločnú databázu (napr. platforma od Tech Against Terrorism s názvom Terrorist Content Analytics Platform [TCAP] alebo databáza na zdieľanie "hashov", ktorú spravuje Globálne internetové fórum na boj proti terorizmu [GIFCT]).

3) Podpora pomocou nahlasovacích systémov

Ak je HSP vystavený teroristickému obsahu - formálne to znamená, že príslušný orgán krajiny, v ktorej sa nachádza hlavné miesto podnikateľskej činnosti HSP alebo jeho právny zástupca, vydal aspoň dva právne záväzné príkazy na odstránenie a HSP bol o tom informovaný - nariadenie o TCO výslovne vyžaduje, aby sa prijali opatrenia na zabránenie ďalšiemu šíreniu takéhoto obsahu (nariadenie o TCO, článok 5.2). Preventívne opatrenia sa odporúčajú aj na preukázanie proaktívneho správania. Jedným z takýchto opatrení môže byť systém nahlasovania, ktorý umožňuje používateľom nahlasovať HSP podozrivý a zakázaný obsah. Má zmysel, aby používatelia určili kategóriu, ktorú by priradili podozrivému obsahu, pričom jednou z takýchto kategórií je terorizmus. To umožní zamestnancom, ktorí spracúvajú hlásenia, rýchlejšie uprednostniť a spracovať obsah podozrivý zo šírenia teroristických myšlienok. Táto predbežná kategorizácia môže uľahčiť aj prípravu neskorších správ o transparentnosti - viac v ► kapitola 6.

4) Pridelenie a preskúmanie ľudskými moderátormi

Označovanie obsahu prostredníctvom automatizovaných nástrojov alebo nahlasovanie jednotlivými používateľmi je prvým krokom pri upozorňovaní na podozrivý, potenciálne nebezpečný obsah. Následne je však zvyčajne potrebné preskúmanie ľudskými moderátormi, kým sa nedosiahne konečné rozhodnutie o opatreniach, ktoré sa majú prijať. Títo moderátori by mali (1) byť dobre oboznámení s predpismi platnými pre platformu, (2) byť schopní rozlíšiť zakázaný obsah od obsahu, ktorý zasahuje do práva na slobodu prejavu, a (3) mať presné znalosti o rôznych možnostiach moderovania na platforme. Je dôležité, aby boli ľudskí moderátori neustále školení o online stratégiách teroristov, ale z etického hľadiska je nemenej dôležité, aby boli poučení o psychologických účinkoch zaobchádzania s problematickým obsahom.

5) Rozhodnutie o tom, ako naložiť s obsahom

Vyššie uvedený proces sa končí rozhodnutím, ako s obsahom naložiť. Môže sa stať, že nebude vykonané žiadne opatrenie a obsah zostane aktívny, ak sa po zvážení všetkých aspektov bude považovať za neškodný. Na druhej strane, v prípade veľmi problematického, nebezpečného alebo inak zakázaného obsahu, ako sú výzvy na teroristické útoky, môže byť obsah a používatelia zablokovaní. Medzi tým však existuje aj množstvo iných spôsobov, ako postupovať v prípade obsahu - obsah, ktorý nepatrí do rozsahu pôsobnosti nariadenia o TCO, si môže vyžadovať diferencovanejšie zaobchádzanie. Podrobnosti a praktické návrhy nájdete v nasledujúcej ► tretej kapitole o účinných stratégiách moderovania.

6) Upozornenie poskytovateľa obsahu

Ak je obsah zablokovaný, musí byť o tom informovaný poskytovateľ obsahu. Na tento účel sa odporúča automatický systém oznamovania a podávania sťažností. Vo všeobecnosti by sa mal na tento účel vytvoriť a nastaviť proces vhodný pre HSP. Podrobnosti a návrhy, ako by sa mohol tento postup uskutočniť v súlade s nariadením o TCO, možno nájsť v ► piatej kapitole.

3. Praktické tipy a rady: Čo pomáha posúdiť, či je obsah nezákonný?

Pokiaľ ide o nariadenie o TCO, HSP nemusia posudzovať zákonnosť obsahu, pretože za to sú zodpovedné príslušné orgány pred vydaním príkazu na odstránenie. **Od HSP sa však vyžaduje, aby proaktívne identifikovali teroristický obsah na svojich platformách, akonáhle boli vystavení teroristickému obsahu.** Často je náročné posúdiť, či obsah prekračuje hranicu zákonnosti, a mal by byť preto zakázaný. Okrem toho by sa nemal zanedbávať psychologický tlak spôsobený prezeraním problematického obsahu. Zamestnanci, ktorí moderujú obsah, by mali mať pravidelné príležitosti na zamyslenie sa nad svojou prácou a v prípade potreby by mali dostať psychologickú podporu.

Na posúdenie nezákonnosti obsahu nájdete nižšie niekoľko tipov a praktických rád. Ešte predtým sa pozrime na príslušné časti o posudzovaní obsahu v nariadení o TCO:

V odseku 11 sa okrem iného uvádza:

> "Pri posudzovaní toho, či materiál predstavuje teroristický obsah v zmysle tohto nariadenia, by príslušné orgány a poskytovatelia hostingových služieb mali zohľadniť také faktory, ako je napríklad povaha a znenie vyhlásení, kontext, v ktorom boli tieto vyhlásenia urobené, ako aj ich potenciál viesť ku škodlivým následkom s vplyvom na bezpečnosť a ochranu osôb." (nariadenie o TCO, 11)

Okrem toho je vždy potrebné zvážiť základné práva:

> "Pri určovaní toho, či materiál, ktorý poskytuje poskytovateľ obsahu, predstavuje „teroristický obsah" vymedzený v tomto nariadení, by sa mala zohľadniť najmä sloboda prejavu a právo na informácie, vrátane slobody a plurality médií a slobody umenia a vedeckého bádania. Najmä v prípadoch, keď poskytovateľ obsahu nesie redakčnú zodpovednosť, by sa pri každom rozhodovaní o odstránení šíreného materiálu mali zohľadňovať novinárske normy stanovené predpismi pre tlač alebo médiá v súlade s právom Únie vrátane charty." (nariadenie o TCO, 12)

Ak HSP dostanú príkaz na odstránenie, príslušný orgán **už obsah klasifikoval ako teroristický**. V **dvoch scenároch je pre HSP užitočné,** aby boli kompetentní a **schopní klasifikovať obsah** ako teroristický alebo neteroristický:

1. Ak HSP ešte nedostal oficiálny príkaz na odstránenie, ale chce konať proaktívne a/alebo presadzovať dodržiavanie svojich vlastných ToS v súvislosti s podozrivým obsahom.
2. Ak HSP dostane oficiálny príkaz na odstránenie, ale má pochybnosti o posúdení obsahu ako teroristického zo strany príslušného orgánu a chce príkaz preskúmať (ako prvý krok k právnemu prostriedku nápravy).

Nižšie nájdete rôzne formy praktickej pomoci pri klasifikácii obsahu ako teroristického alebo neteroristického.

Používanie zoznamov označení

Národné a medzinárodné zoznamy, ktoré pomenúvajú teroristické organizácie, poskytujú dobrý rámec a referenčný bod pre klasifikáciu obsahu. Napríklad prijatie zoznamov označení ako základu pre zákaz alebo blokovanie, na ktoré by sa malo odkazovať v ToS (▶kapitola 1), dáva sankciám platformy oporu v zákone. V odseku 11 nariadenia o TCO sa výslovne navrhuje, že pri posudzovaní obsahu sa môže použiť zoznam Európskej únie.

Využívanie databáz kľúčových slov, symbolov a loga

Ľudia, ktorí manuálne kontrolujú obsah, by mali mať k dispozícii nielen definíciu teroristického obsahu, ale mali by tiež poznať a udržiavať si znalosti kľúčových slov a fráz, ktoré zvyčajne používajú teroristické organizácie. Čím intenzívnejšie je osoba posudzujúca obsah oboznámená s teroristickým fenoménom (napr. pravicový, ľavicový, islamistický), tým ľahšie rozpozná taktiku zastierania, ako je tzv. dog whistling, t. j. používanie zdanlivo neškodných slov, ktoré majú v rámci scény ideologický význam . Databáza log a symbolov, t. j. vizuálnych prvkov, ktoré naznačujú teroristické pozadie, je rovnako nevyhnutná na presné a rýchle posúdenie obsahu.

Zahrnutie kontextových faktorov

Moderovanie by malo zohľadňovať kontext, v ktorom bol obsah pravdepodobne uverejnený. Medzi relevantné kontextové faktory patria okrem iného (a) politické podmienky, (b) aktuálne udalosti vrátane nedávneho vývoja v spravodajstve a (c) kultúrne okolnosti, ktoré môžu formovať názory na určité otázky. Často je to ťažké posúdiť - najmä ak sú používatelia anonymní a obsah, ktorý zverejňujú, obsahuje len málo alebo žiadne textové indície o ich identite - ale v niektorých prípadoch, keď sa v obsahu uvádzajú vonkajšie faktory, sa ukazuje, že úvahy o kontexte sú užitočné.

Okrem toho, ak ide o obsah, ktorý **nie je teroristický, ale škodlivý iným spôsobom** (napr. rôzne formy nenávistných prejavov), možno zvážiť tieto body.

Zváženie rozsahu potenciálnych škôd spôsobených obsahom

Teroristický, extrémistický a ďalší škodlivý obsah, ako sú nenávistné prejavy alebo podnecovanie k násiliu, najmä ak podnecujú k páchaniu teroristických trestných činov, môže spôsobiť značné škody. Pri posudzovaní obsahu môže byť užitočné zohľadniť rozsah, v akom môže byť obsah príčinným faktorom takejto škody. Čím väčšia škoda môže vzniknúť, tým rýchlejšie a premyslenejšie treba konať. Nepriaznivé psychologické účinky na osoby, ktorých sa škodlivý obsah dotýka, by sa mali považovať za formu škody.

Zváženie potenciálneho vplyvu odstránenia obsahu

Nariadenie o TCO vyzýva na citlivé vyváženie základných práv zakotvených v charte (napr. sloboda prejavu a informácií) pri posudzovaní odstránenia obsahu. Ak odstránenie nenariadil príslušný orgán, existujú iné spôsoby, ako možno so škodlivým obsahom zaobchádzať - ich príklady nájdete v ▶kapitola 3.

4. Čo mám robiť, ak to vidím inak? Ako namietať proti prijatému príkazu na odstránenie

Čo treba urobiť, keď si posúdenia HSP a príslušného orgánu odporujú?

HSP, ako aj poskytovateľ obsahu majú právo napadnúť príkaz na odstránenie podľa článku 9 nariadenia o TCO. Toto právo je dôležitou kontrolou a rovnováhou, ktorá dokáže zachovať základné práva.

Námietky proti príkazom na odstránenie sa podávajú na súdoch členského štátu EÚ, ktorého príslušný orgán odstránenie nariadil. **HSP sú povinní uchovávať v bezpečných podmienkach a po dobu šiestich mesiacov všetok obsah, ktorý bol odstránený (buď v dôsledku príkazu na odstránenie, alebo iných opatrení), ako aj všetky údaje súvisiace s obsahom (napr. čas uverejnenia, informácie o účte)**. Tým sa napomáha vyšetrovaniu a predchádzaniu teroristickým trestným činom alebo hrozbám a zabezpečuje sa dostatok času na začatie právnych sporov proti odstráneniu obsahu a v prípade potreby na obnovenie obsahu (nariadenie o TCO, 27 a 28).

Špecifický prípad: Cezhraničné príkazy na odstránenie (nariadenie o TCO, Článok 4)

Ak HSP dostane príkaz na odstránenie od príslušného orgánu v inom členskom štáte EÚ, ako je jeho "domovský orgán" (t. j. príslušný orgán členského štátu, v ktorom má HSP hlavné miesto podnikateľskej činnosti alebo právneho zástupcu; podrobnosti o právnych zástupcoch sú uvedené v ►kapitole 4), **uplatňuje sa osobitný postup.**

Pri vydávaní príkazu na odstránenie musí príslušný orgán zaslať kópiu tohto príkazu aj "domovskému orgánu", ktorý má 72 hodín na preskúmanie príkazu. Ak sa zistí, že príkaz na odstránenie porušuje základné práva a slobody zakotvené v charte, môže vydať odôvodnené rozhodnutie, ktoré môže znamenať námietku.

HSP musí po doručení príkazu na odstránenie odstrániť a zaistiť obsah (rovnako ako v prípade príkazu na odstránenie vydaného "domovským orgánom"). HSP (a poskytovateľ odstráneného obsahu) môže do 48 hodín podať žiadosť o preskúmanie "domovskému orgánu", ktorý je oprávnený preskúmať príkaz na odstránenie a odpovedať na ňu do 72 hodín od prijatia žiadosti, pričom o preskúmaní informuje príslušný orgán, ktorý pôvodne nariadil odstránenie.

Po vydaní odôvodneného rozhodnutia orgánom, ktorý preskúmanie nariadil, sú o tom informované príslušné subjekty (konkrétne pôvodný orgán, HSP, poskytovateľ obsahu a prípadne Europol) a v prípade zistenia porušenia môže HSP obsah okamžite obnoviť.

Kapitola 3

Zavádzanie účinných mechanizmov moderovania teroristického obsahu online

Zhrnutie: Obsah a hlavné body tejto kapitoly

- Pri moderovaní obsahu sa **obsah používateľa preskúmava s cieľom posúdiť, či boli dodržané alebo porušené právne predpisy** (napr. Nariadenie o TCO, DSA) **a pravidlá špecifické pre platformu** (napr. ToS).
- **Ak bolo pravidlo porušené, obsah bude "moderovaný".** Inými slovami, prijmú sa opatrenia na obmedzenie jeho dosahu.
- Ak príslušný orgán dostane **príkaz na odstránenie** na základe nariadenia o TCO, **moderovanie obsahu vždy zahŕňa odstránenie** príslušného teroristického obsahu, hoci HSP a používatelia to môžu napadnúť, ak s tým nesúhlasia.
- Pred prijatím opatrení na moderovanie zo strany HSP, počas neho alebo krátko po ňom, ako aj pri neskoršom preskúmaní je potrebné zohľadniť rôzne body. Patrí k nim oznámenie používateľom, ktorých obsah bol moderovaný, a možnosť odvolať sa proti rozhodnutiu.
- Ak platformy prijímajú **proaktívne opatrenia proti iným potenciálne škodlivým formám obsahu**, ako sú nenávistné prejavy alebo urážky, bez ohľadu na nariadenie o TCO, možno zvážiť aj iné **alternatívne prístupy k moderovaniu**.

1. Čo je moderovanie obsahu a prečo je v niektorých prípadoch potrebné?

Moderovanie obsahu zahŕňa **preskúmanie obsahu vytvoreného používateľom** (UGC) na internete s cieľom **posúdiť vhodnosť** obsahu na základe pravidiel platformy (napr. ToS) a právnych rámcov (napr. nariadenie TCO, DSA)[3]. **Pravidlá platforiem a právne požiadavky sa presadzujú prostredníctvom moderovania obsahu**, aby sa prijali potrebné opatrenia proti zakázanému a/alebo problematickému obsahu. Od HSP sa vyžaduje, aby boli transparentní, pokiaľ ide o konkrétne opatrenia prijaté na identifikáciu a odstránenie teroristického obsahu vrátane proaktívnych a reaktívnych procesov moderovania obsahu a všetkých používaných automatizovaných nástrojov.

Moderovanie obsahu je veľmi dôležitý, ale aj veľmi komplikovaný a **citlivý** postup. Disponovanie vhodnými technickými a odbornými zdrojmi môže byť pre menšie spoločnosti značnou finančnou záťažou. Okrem toho teroristický obsah môže byť vytvorený vo všetkých jazykoch a je mimoriadne nákladné zabezpečiť, aby moderátori boli schopní posúdiť obsah vo všetkých týchto jazykoch.

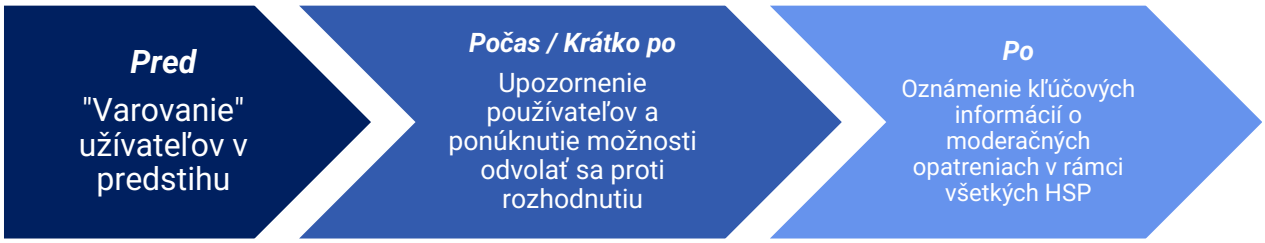
[3] Roberts, S.T. (2017). Content Moderation. In L. Schintler & C. McNeely (eds.): *Encyclopedia of Big Data*. Springer, Cham. https://doi.org/10.1007/978-3-319-32001-4_44-1

Základné práva zakotvené v Deklarácii OSN o ľudských právach, najmä právo na slobodu prejavu, sa musia vždy porovnať so škodou spôsobenou príslušným obsahom. Na druhej strane majú HSP spoločenskú zodpovednosť za zmiernenie škodlivého obsahu na svojich platformách.

Zrozumiteľná a transparentná moderácia obsahu pomáha chrániť používateľov a zainteresované strany pred účinkami škodlivého obsahu a buduje dôveru. Z pohľadu HSP môže moderovanie obsahu posilniť obmedzovanie zodpovednosti, dodržiavanie platných zákonov a ochranu pred poškodením dobrej povesti spôsobeným zneužitím platformy.

Moderovanie obsahu nemusí nevyhnutne znamenať odstránenie obsahu. Hoci odstránenie obsahu môže byť povinné z dôvodu zákonných požiadaviek - ako je to v prípade príkazov na odstránenie na základe nariadenia o TCO - existujú aj iné spôsoby, ako sa vysporiadať so škodlivým obsahom. V závislosti od toho, aký problematický a závažný je obsah a aké škody môže spôsobiť, možno zvážiť alternatívne možnosti. Príklady a návrhy alternatívnych stratégií moderovania nájdete v ▶časti 3 tejto kapitoly.

Štýly moderovania sa líšia od platformy k platforme v závislosti od ich funkcionalít, ponúkaných služieb, hodnôt platformy a tolerancie rizika[4]. Pri moderovaní obsahu je dôležité byť čo najtransparentnejší. To zahŕňa rôzne faktory, ktoré je potrebné zohľadniť pred moderovaním, počas neho a po ňom, aby používatelia vedeli, aké moderátorské zásahy môžu byť vykonané v súvislosti s ich obsahom.



1. **Pred:** "Varovanie" užívateľov v predstihu

Už v počiatočnej fáze informujte používateľov o tom, k akým opatreniam na úpravu obsahu môže dôjsť v dôsledku správania alebo uverejnenia obsahu, ktorý je zakázaný podľa ToS alebo podľa zákona. To znamená: zahrňte informácie o svojich stratégiách moderovania do záväznej dohody s používateľmi, t. j. do ToS (▶kapitola 1). Pomáha to tiež zabezpečiť, aby ste si začali budovať dôveru s jednotlivcami ešte pred alebo v čase nadviazania vzťahu s používateľom a aby ste poskytli záväzné

[4] Roberts, S.T. (2017). Content Moderation. In L. Schintler & C. McNeely (eds.): *Encyclopedia of Big Data*. Springer, Cham. https://doi.org/10.1007/978-3-319-32001-4_44-1

a jednoznačné uistenie, že problematický a nezákonný obsah nebude na platforme tolerovaný a že ako HSP chcete používateľov pred takýmto obsahom chrániť.

2. **Počas (alebo krátko po činnosti):** Upozornenie používateľov, ktorých obsah bol zablokovaný alebo moderovaný, a ponúknutie možnosti odvolať sa proti rozhodnutiu.

Článok 11 nariadenia o TCO zaväzuje HSP, aby v prvom rade informovali používateľa, ktorý poskytol (t. j. vytvoril a/alebo nahral) zakázaný (teroristický) obsah, že bol platformou zablokovaný, a v druhom rade, aby používateľovi na jeho žiadosť poskytli informácie o pozadí alebo príkaz na odstránenie. Oznámenie možno poskytovateľom obsahu dočasne odoprieť na obdobie najviac šiestich týždňov, ak sa príslušný orgán domnieva, že s oznámením o odstránení poskytovateľovi obsahu je spojené osobitné nebezpečenstvo. Ak je nezverejnenie stále dôležité a vhodné, príslušný orgán môže predĺžiť obdobie o ďalších šesť týždňov (nariadenie o TCO, Článok 11.3). Nariadenie o TCO (Článok 10) poskytuje osobitné mechanizmy na riešenie takýchto situácií. Odporúča sa zaviesť štandardizovaný automatický proces, prostredníctvom ktorého budú poskytovatelia obsahu informovaní o vymazaní a budú mať možnosť podať proti nemu sťažnosť. Tento mechanizmus oznamovania a podávania námietok by sa mal zaviesť aj v prípadoch, na ktoré sa nevzťahuje nariadenie o TCO, ale ktoré sa uskutočnili prostredníctvom (pro)aktívnych opatrení zo strany HSP.

3. **Po:** Pravidelne verejne oznamovať kľúčové údaje o opatreniach na moderovanie obsahu v rámci všetkých HSP.

Transparentnosť rozhodnutí o moderovaní obsahu a jeho výsledkov je dôležitá na vytvorenie dôvery a zodpovednosti medzi HSP a ich používateľmi a čoraz častejšie ju nariaďujú rôzne typy online predpisov. Správy o transparentnosti zachytávajú informácie o rozhodnutiach platforiem o moderovaní, a to nielen o počte a type zistených porušení, ale aj o tom, ako presne boli tieto porušenia riešené. (Podrobnejšie informácie o správach o transparentnosti a požiadavkách na transparentnosť TCO nájdete v ▶kapitole 6.)

2. Praktické tipy a rady: Ako by sa malo vykonávať moderovanie obsahu?

Je dôležité, aby HSP mali jasný **proces moderovania obsahu**, ktorý sa dá prispôsobiť konkrétnym obchodným službám a potrebám. Je veľmi dôležité najprv identifikovať zakázaný obsah a vedieť posúdiť jeho nezákonnosť, ako sa podrobnejšie uvádza v ▶kapitole 2. Pripomeňme si tieto hlavné kroky:

1. Definícia teroristického obsahu
2. Podpora pomocou automatizovaných nástrojov
3. Podpora zo systémov podávania správ
4. Pridelenie a preskúmanie ľudskými moderátormi
5. **Rozhodnutie o tom, ako naložiť s obsahom (t. j. rozhodnutie o moderácii obsahu)**
6. Oznámenie poskytovateľovi obsahu

V tejto časti sa zaoberáme ***krokom 5***. V ▶kapitole 2, sme tento krok nazvali "Rozhodnutie o tom, ako naložiť s obsahom". Po prijatí príkazu na odstránenie obsahu od príslušného orgánu musia HSP obsah odstrániť a majú možnosť sa proti príkazu odvolať. HSP sa môžu rozhodnúť aj o aktívnej identifikácii a odstránení teroristického alebo zakázaného obsahu (t. j. bez príkazu na odstránenie).

V tejto príručke sa rozlišuje päť rôznych typov moderácie: predbežná, následná, reaktívna, distribuovaná a automatizovaná. Stručné vysvetlenie každej z nich, ako aj ich výhody a nevýhody nájdete nižšie.

Typ moderovania	Vysvetlenie
Predbežná moderácia	Moderátori skontrolujú obsah pred jeho zverejnením. **Výhody:** Vysoký stupeň bezpečnosti a súladu obsahu s právnymi normami a predpismi špecifickými pre platformu **Nevýhody:** Vysoké nároky na úsilie, personál a (prípadné) finančné náklady
Následná moderácia	Moderátori skontrolujú obsah bezprostredne po zverejnení. **Výhody:** Umožnenie rýchlej interakcie používateľa s obsahom (vďaka okamžitému zverejneniu) **Nevýhody:** Značné množstvo času, personálnych (prípadne) finančných nákladov; v prípade zakázaného/škodlivého obsahu sú používatelia vystavení tomuto obsahu
Reaktívna moderácia	Moderátori skontrolujú obsah po tom, čo ho používatelia nahlásili. **Výhody:** Menšia náročnosť na zdroje HSP; budovanie dôvery u používateľov (prostredníctvom možnosti nahlasovania obsahu) **Nevýhody:** Zodpovednosť používateľov; v prípade zakázaného/škodlivého obsahu sú používatelia stále vystavení obsahu; možnosť falošných poplachov, ktoré si vyžadujú dodatočné úsilie zo strany HSP
Distribuovaná moderácia	Komunita používateľov pôsobí ako moderátori, často prostredníctvom mechanizmu hodnotenia, ktorým sa meria dôveryhodnosť obsahu a ktoré sa v konečnom dôsledku používa na určenie verejného dosahu obsahu (t. j. obsah s vyššími hodnoteniami sa umiestňuje lepšie a má väčší dosah). **Výhody:** Menšia náročnosť na zdroje zo strany HSP; podpora zapojenia používateľa; samoregulácia **Nevýhody:** Zodpovednosť používateľov; v prípade zakázaného/škodlivého obsahu sú používatelia vystavení obsahu; náchylnosť na koordinované manipulatívne správanie zo strany zlomyseľných používateľov

Automatizovaná moderácia	Modely založené na umelej inteligencii (napr. filtre, algoritmy) fungujú ako moderátory. **Výhody:** Po nastavení je menej náročný na zdroje; včasná, rýchla a vysoko škálovateľná detekcia potenciálne škodlivého obsahu **Nevýhody:** Náchylnosť na chyby, najmä pokiaľ ide o chybné vymazanie obsahu (problematické v kontexte slobody prejavu, preto je dôležité ľudské hodnotenie); potrebná neustála údržba a prispôsobovanie sa novému vývoju

(Podľa Grimes-Viort, 2010)[5]

Odporúča sa kombinovať niekoľko prístupov k moderovaniu obsahu. Reaktívna moderácia sa dá napríklad ľahko kombinovať s predbežnou alebo následnou moderáciou. Vo väčšine prípadov sú **kombinácie veľmi užitočné a v niektorých prípadoch môžu byť dokonca nevyhnutné**. Automatizované rozhodnutia o moderovaní musia byť vždy preskúmané alebo aspoň založené na ľudskej kontrole, aby sa predišlo systematickému porušovaniu základných práv používateľov a ohrozeniu slobody prejavu.

Pamätajte, že extrémistickí a teroristickí aktéri môžu používať **taktiky, aby sa vyhli známym metódam moderovania obsahu**, pôsobili nenápadne, a tak obchádzali moderovanie, najmä automatické mechanizmy moderovania obsahu. Medzi obľúbené taktiky patrí používanie *skracovania adries URL* s cieľom vyhnúť sa filtrom alebo blokovaniu webových stránok, *zrkadlenie* účtov a obsahu, ktoré zahŕňa viacnásobné zverejňovanie alebo vytváranie identického obsahu/účtov s cieľom zahltiť moderátorov a mať k dispozícii záložné kópie pre prípad vymazania, alebo *zámerné vyberanie (nesprávnych) pravopisných tvarov slov*, aby sa vyhli automatickým filtrom slov. Rozsah obchádzajúcich techník zdôrazňuje dôležitosť ľudského moderovania.

Vaša účasť na tejto príručke alebo vaša (certifikovaná) účasť na online kurze, ktorý je tiež ponúkaný ako súčasť projektu TATE, svedčí o tom, že sa o tieto trendy zaujímate. Ďalšie príklady vyhýbania sa moderovaniu obsahu, ako aj uskutočniteľné a účinné reakcie nájdete v platforme na zdieľanie znalostí Tech Against Terrorism, ktorá je k dispozícii na tomto odkaze.

3. Alternatívne prístupy k moderovaniu

Moderovanie nemusí vždy znamenať vymazanie obsahu. Alternatívne prístupy, ktoré sú navrhnuté nižšie, môžu byť zaujímavé pre HSP, ktorí sa snažia (pro)aktívne moderovať obsah nad rámec požiadaviek nariadenia o TCO. Je dôležité zdôrazniť, že takéto alternatívne prístupy k moderovaniu **nepatria do rozsahu pôsobnosti nariadenia o TCO a možno ich použiť len vtedy, keď platformy nedostali príkaz na odstránenie, ale chcú proaktívne moderovať neteroristický, inak škodlivý obsah**. Keď dostanete príkaz na odstránenie, postup je jasný: obsah musíte odstrániť a žiadne alternatívne prístupy k moderovaniu neprichádzajú do úvahy.

[5] Grimes-Viort, B. (2010, December 7). 6 types of content moderation you need to know about. *Social Media Today*. https://www.socialmediatoday.com/content/6-types-content-moderation-you-need-know-about

CHCETE UROBIŤ VIAC PRE BEZPEČNOSŤ SVOJEJ PLATFORMY?

Skrytie obsahu

HSP môžu čiastočne alebo úplne skryť obsah, a tým sa vyhnúť jeho blokovaniu, ak sa domnievajú, že používatelia môžu považovať obsah za urážlivý alebo nevhodný, ale napriek tomu je legitímny, legálny a povolený v rámci celej platformy. Skrývanie obsahu pred ľuďmi zo zraniteľnej skupiny alebo ľuďmi nachádzajúcimi sa v krajine, kde je obsah nezákonný (zatiaľ čo v iných krajinách je povolený), je jednou z takýchto reakcií. Na skrytie obsahu možno použiť rôzne technické funkcie, ako napríklad filtre na prihlasovanie alebo platenie, zabezpečený režim (vyhľadávania) na zobrazenie obsahu vhodného pre vekovú kategóriu alebo geografické, či časové blokovanie.

Oddelenie obsahu od mechanizmov odmeňovania ("odpojenie")

Oddeľovanie oberá určitý obsah alebo používateľov o metriky zapojenia, odrádza od aktivity okolo príspevku a môže spôsobiť, že obsah sa vo všeobecnosti nebude vyplácať zverejňovať. Obsah a používateľské konto však zostávajú na platforme. Odpojenie obmedzuje významnosť príspevkov alebo účtov na platforme. Medzi typické taktiky odpojenia patrí deaktivácia funkcií platformy, ako je v prípade mnohých sociálnych sietí možnosť lajkovať, komentovať alebo zdieľať príspevky, takže príspevok možno len čítať, demonetizácia (t. j. zbavenie účtov možnosti zarábať na svojom obsahu) alebo deverifikácia (t. j. odstránenie akéhokoľvek osvedčenia identity účtu alebo používateľa). Takéto sankcie môžu mať za následok zmenu zaobchádzania s obsahom alebo účtom zo strany algoritmu platformy a môžu sa kumulovať: zníženie hodnotenia obsahu znamená, že je ťažšie ho rozšíriť a propagovať prostredníctvom mechanizmov platformy (zvyčajne odporúčacích algoritmov).

Pripojenie pedagogických poznámok k obsahu

Cieľom pedagogických alebo komunikačných taktík je ponúknuť používateľom dodatočné informácie, aby sa nakoniec mohli sami rozhodnúť, či chcú daný obsah vidieť alebo nie. Nakoniec platforma rozhoduje o tom, ktorý obsah je opatrený takýmito poznámkami, čo tieto poznámky zahŕňajú, pred akou kategóriou poškodenia sú používatelia varovaní a koľko dodatočných informácií sa ponúka. Známou praxou, ktorú predtým používal (predchádzajúci) Twitter, je upozornenie používateľov, že v príspevku sa môže nachádzať škodlivý obsah, napríklad dezinformácie alebo konšpiračné príbehy, a umožňuje používateľom vidieť tento obsah až po tom, ako aktívne potvrdia, že si to želajú, kliknutím na tlačidlo. Najmä v prípade politicko-ideologického obsahu, ktorý by mohol podporovať radikalizáciu, môžu kontra informácie a odkazy na vzdelávacie informácie upozorniť ľudí na možné účinky takéhoto obsahu.

Prenechanie zodpovednosti používateľom ("posilnenie postavenia komunity")

Predpokladom mechanizmov moderovania obsahu založených na posilnení postavenia komunity je umožniť samotným používateľom vytvárať digitálny priestor

> podľa ich predstáv. Takéto stratégie môžu byť zaujímavé najmä pre platformy, kde je dôležitá myšlienka komunity alebo ktorých moderátorské postupy už do istej miery závisia od podpory používateľov. Tieto moderátorské prístupy sledujú typ distribuovanej moderácie. Okrem už spomínanej funkcie zvyšovania a znižovania hodnoty obsahu hlasovaním, sem patrí aj individuálne blokovanie alebo stlmovanie konkrétnych účtov, ktoré už ponúka veľký počet platforiem, alebo využívanie administrátorov či moderátorov zo samotnej komunity. S tým úzko súvisí aj koncepcia "dôveryhodných nahlasovateľov", ktorá je rozoberaná v DSA (Článok 22). Tento pojem sa vzťahuje na používateľov, ktorí sú obzvlášť dôveryhodní a kompetentní posúdiť nezákonnosť obsahu a nahlásiť ju (objektívne a rýchlo) a ktorí zastupujú kolektívne záujmy (orientované na verejné blaho) bez ohľadu na konkrétnu online platformu. Takto nahlásený obsah by mal byť na strane HSP spracovaný prioritne a rýchlo.

Tieto alternatívne prístupy k moderovaniu môžu byť relevantné aj v prípadoch, keď platformy nie sú na základe nariadenia o TCO nútené prijať opatrenia. Bez ohľadu na to, akú formu má, nariadenie o TCO umožňuje proaktívny prístup: ak sa v priebehu (pro)aktívnych vlastných moderátorských opatrení HSP stretne s obsahom, ktorý sa týka bezprostredného ohrozenia života alebo teroristického činu, musí ho vymazať a bezodkladne o tom informovať príslušný orgán členského štátu EÚ, ktorého sa to týka (nariadenie o TCO, článok 14.5).

Podrobnejšie informácie o (technických) metódach, ktoré si tieto alternatívne prístupy vyžadujú, ako aj o ich výhodách a nevýhodách a prípadových štúdiách poskytuje organizácia Tech Against Terrorism na tomto odkaze.

Kapitola 4

Zriadenie kontaktných miest a právnych zástupcov

Zhrnutie: Obsah a hlavné body tejto kapitoly

- Nariadenie o TCO rozlišuje medzi kontaktnými miestami a právnymi zástupcami.
- **Kontaktné miesta musia byť zriadené každým HSP** a sú **zodpovedné za** prijímanie **príkazov na odstránenie** a ich rýchle spracovanie.
- **Ak HSP nie sú usadení v EÚ, musí byť určený aj právny zástupca.** Táto osoba je zodpovedná za prijímanie, dodržiavanie a presadzovanie nariadenia o TCO. Právny zástupca môže, ale nemusí súčasne pôsobiť ako kontaktné miesto.
- Každý HSP bez ohľadu na to, či bol vystavený teroristickému obsahu, musí zriadiť kontaktné miesto a v prípade potreby aj právneho zástupcu podľa nariadenia TCO.

Nariadenie o TCO stanovuje, že *všetci* HSP, ktorých sa toto nariadenie týka (t. j. podľa definície spadajú do rozsahu pôsobnosti nariadenia; ▶ viď časť o dotknutých platformách v úvode), sú povinní určiť kontaktné miesto alebo právneho zástupcu.

1. Čo sú kontaktné miesta a právni zástupcovia?

Kontaktné miesto (nariadenie o TCO, 42 a Článok 15)

- **Účel**: Kontaktné miesta HSP uľahčujú okamžité spracovanie príkazov na odstránenie. Kontaktné miesto preto slúži len na operatívne účely.
- **Logistika**: Kontaktné miesto by malo byť schopné prijímať a odosielať príkazy na odstránenie elektronicky bez ohľadu na to, či sa nachádza v rámci organizácie alebo je externe zabezpečené.
- **Potrebné zdroje**: Kontaktné miesto musí mať dostatočné technické možnosti, prístup a musí byť personálne vybavené tak, aby sa príkazy na odstránenie mohli spracovať bezodkladne. Keďže teroristický obsah sa musí odstrániť do jednej hodiny od prijatia príkazu na odstránenie, znamená to, že kontaktné miesto musí byť k dispozícii 24 hodín denne, 7 dní v týždni.
- **Lokalizácia**: Kontaktné miesto sa nemusí nevyhnutne nachádzať v EÚ.
- **Komunikácia**: V informáciách o dostupnosti kontaktného miesta by mal byť uvedený jazyk, v ktorom prebieha komunikácia. S cieľom umožniť komunikáciu medzi HSP a príslušnými orgánmi členských štátov by sa mal používať aspoň jeden úradný jazyk EÚ. Mal by to byť jazyk, v ktorom sú k dispozícii aj ToS platformy.

Právny zástupca (nariadenie o TCO, Článok 17)

- **Nevyhnutnosť**: Ak HSP nemá hlavné miesto podnikateľskej činnosti v EÚ, musí byť určený právny zástupca. Ide o fyzickú alebo právnickú osobu, ktorá sa nachádza v jednom z členských štátov EÚ, v ktorom HSP ponúka svoje služby.
- **Účel**: Tento právny zástupca je zodpovedný za prijímanie, dodržiavanie a presadzovanie nariadenia o TCO a najmä príkazov na odstránenie.
- **Zdroje**: HSP musia poskytnúť právnym zástupcom právomoci, kapacity a zdroje na dodržiavanie nariadenia o TCO a na spoluprácu s príslušnými orgánmi.
- **Zodpovednosť**: Právni zástupcovia môžu niesť zodpovednosť za porušenie nariadenia o TCO.
- **Vzťah s kontaktným miestom**: Právny zástupca môže zároveň pôsobiť aj ako kontaktné miesto, ale nie je povinný tak robiť.

2. Prečo je potrebné mať kontaktné miesto alebo právneho zástupcu?

V iných kapitolách sa hovorí o viacerých možnostiach, ktoré môžu byť pre HSP atraktívne aj z obchodného hľadiska, ale hlavným dôvodom a argumentom na **zriadenie kontaktného miesta alebo určenie právneho zástupcu je to, že je to povinné**. Môže si to vyžadovať určité prerozdelenie zdrojov, ale je nepochybne v najlepšom záujme HSP dodržiavať zákon a vyhnúť sa negatívnym dôsledkom jeho nedodržania, ako je strata dobrého mena, dôvery a finančných prostriedkov v prípade uloženia pokuty, tým, že sa ustanovenie vykoná bezodkladne.

HSP musia umožniť príslušným orgánom preskúmať informácie o kontaktnom mieste a následne poskytovať elektronické oznámenia (t. j. podať príkaz na odstránenie elektronicky). Zvyčajne to zahŕňa poskytnutie e-mailovej adresy (napríklad v časti " Kontaktujte nás" na webovom sídle HSP), prostredníctvom ktorej sa príslušný orgán môže obrátiť na kontaktné miesto.

Pri vymenovaní právneho zástupcu je potrebné zdôrazniť dva aspekty. Po prvé, **totožnosť právneho zástupcu musí byť zverejnená** (pozri kontaktné miesto). Po druhé, **HSP musí aktívne oznámiť vymenovanie svojmu "domovskému orgánu"** (t. j. príslušnému orgánu členského štátu, v ktorom má právny zástupca sídlo).

Europol tiež vytvoril platformu, Plateforme Européenne de Retraits de Contenus illicites sur Internet (Európska platforma na odstraňovanie nezákonného obsahu na internete) alebo PERCI **na podporu vykonávania nariadenia o TCO**. Účelom PERCI je zabezpečiť, aby HSP mohli prijímať príkazy na odstránenie z členských štátov prostredníctvom spoločného zabezpečeného kanála namiesto 27 samostatných systémov pre každý členský štát. Zefektívňuje príkazy na odstránenie z rôznych členských štátov a funguje ako jednotné kontaktné miesto v súvislosti s nahlasovaniami a príkazmi na odstránenie a má zabrániť duplicite príkazov na odstránenie, t. j. tomu, aby ten istý príkaz zaslali dva členské štáty. Pre HSP je tiež užitočné mať centralizovaný príjem príkazov na odstránenie a nahlásení prijatých v priebehu času, aby sa podporila povinnosť podávať správy o transparentnosti. Prostredníctvom PERCI môžu HSP tiež požiadať o kontrolu a preskúmanie s cieľom napadnúť príkaz na odstránenie

3. Čo je príslušný orgán členského štátu EÚ a ako ho môžem kontaktovať?

Za určitých okolností je potrebné kontaktovať príslušný orgán v súvislosti s právnym zástupcom. Jedna z takýchto "okolností" nastáva pri napadnutí príkazu na odstránenie. Iným príkladom môže byť prípad, keď sa HSP dozvie o teroristickom obsahu zahŕňajúcom bezprostredné ohrozenie života alebo ak sa jedná o teroristický čin bez príkazu na odstránenie. V takom prípade je HSP povinný ho okamžite vymazať a informovať o tom príslušný orgán členského štátu EÚ, ktorého sa týka (nariadenie o TCO, článok 14.5).

Väčšina príslušných orgánov členských štátov EÚ už zriadila kontaktné miesta. Aktuálny zoznam vrátane kontaktných údajov nájdete na webovej stránke Európskej komisie tu.

Kapitola 5

Nastavenie systému upozornení a sťažností používateľov na odstránený obsah

Zhrnutie: Obsah a hlavné body tejto kapitoly

- Dotknutí **používatelia môžu využiť postupy podávania sťažností, aby sa odvolali proti príkazom na odstránenie** (a v prípade potreby a nad rámec nariadenia o TCO aj iné proaktívne moderačné opatrenia).
- Postupy podávania sťažností sú dôležité ako **kontrolný mechanizmus a mechanizmus spätnej väzby** z hľadiska používateľov, spoločností a práva.
- HSP "zavedú účinné a prístupné" systémy podávania sťažností (nariadenie o TCO, Článok 10.1).
- Podľa nariadenia o TCO musia systémy na podávanie sťažností spĺňať určité obsahové a technické požiadavky.
- Postup podávania sťažností môže mať dva rôzne výsledky, a to (1) sťažnosti sa vyhovie, pretože sa zistí, že obsah bol zablokovaný neoprávnene, alebo (2) sťažnosť sa zamietne, pretože sa zistí, že obsah bol zablokovaný oprávnene.
- V závislosti od výsledku procesu podávania sťažností môže byť obsah predmetom ďalších opatrení.
- V tejto kapitole sa okrem toho uvádzajú usmernenia k navrhovaniu a realizácii postupu podávania sťažností špecifického pre HSP.

Postupy podávania sťažností umožňujú používateľom odvolať sa proti odstráneniu obsahu prostredníctvom komunikácie s platformou a **sú prvým krokom k (právnemu) napadnutiu príkazu na odstránenie**. Viac informácií o procese riešenia sporov nájdete v ▶kapitole 2.

1. Prečo je potrebné vytvoriť transparentný systém podávania sťažností?

Je dôležité vytvoriť systém podávania sťažností, a to najmä z a) právneho hľadiska, b) hľadiska používateľov a c) hľadiska spoločnosti.

a) Právne hľadisko

Postupy podávania sťažností sú v súlade s **právnymi predpismi, na základe ktorých sú takéto mechanizmy potrebné**. Napríklad v nariadení o TCO (nariadenie o TCO, článok 10) sa stanovuje, že HSP musia zaviesť účinný a dostupný systém podávania sťažností, aby používatelia mali možnosť napadnúť odstránenie alebo zablokovanie obsahu po osobitnom opatrení. Podľa nariadenia o TCO musí byť poskytovateľ obsahu informovaný o konečnom výsledku do dvoch týždňov.

b) Hľadisko používateľa

Systém podávania sťažností nie je len zákonnou požiadavkou. Jasný a prístupný mechanizmus podávania sťažností pomáha budovať dôveru používateľov - tých, ktorých obsah bol moderovaný, ale predovšetkým neovplyvnených používateľov, ktorí platformu používajú podľa jej účelu. Týmto spôsobom HSP preukazujú, že používatelia sa môžu spoľahnúť na procesy moderovania, že tieto procesy sú založené na pocite **zodpovednosti voči používateľom** a že platformy berú ohľad na **základné práva**, ako je sloboda prejavu a informácií.

c) Hľadisko spoločnosti

Systémy podávania sťažností môžu byť užitočnou formou **sebakontroly**, pri ktorej možno posúdiť účinnosť, spravodlivosť a konzistentnosť moderátorských opatrení a noriem. Takéto systémy môžu poskytnúť záruku, že vaša platforma sa používa tak, ako má, čo ďalej pomáha chrániť **dobré meno** online služieb a ďalej chrániť právo na slobodu prejavu online.

2. Aké sú požiadavky na systémy podávania sťažností?

Podľa nariadenia o TCO (33 a článok 10) by systémy podávania sťažností mali byť:

- užívateľsky prívetivé,
- účinné a (ľahko) dostupné,
- poskytnúť bezpečný rámec, v ktorom sa sťažnosti riešia rýchlo a transparentne, aby bol sťažovateľ do dvoch týždňov informovaný o výsledku preskúmania.

Systém podávania sťažností musí byť nastavený na účely nariadenia o TCO tak, aby bolo možné obnoviť chybne odstránený obsah. Sťažnosti však možno podávať aj proti opatreniam prijatým na presadzovanie ToS platformy nad rámec nariadenia o TCO.

3. Ako sa majú sťažnosti vybavovať a aké sú možné výsledky?

Po zavedení systému podávania sťažností a podaní sťažnosti používateľom, HSP **sťažnosť preskúma** a **oznámi rozhodnutie sťažovateľovi najneskôr do dvoch týždňov v prípadoch, na ktoré sa vzťahuje nariadenie o TCO**.

Existujú dva možné výsledky procesu preskúmania, ktoré sú uvedené v nasledujúcej tabuľke.

Výsledok A **Sťažnosť používateľa proti odstráneniu obsahu bola potvrdená**	*Výsledok B* **Sťažnosť používateľa proti odstráneniu obsahu zamietnutá**
Výsledok: Sťažnosť proti odstráneniu obsahu je **opodstatnená**, a preto sa jej vyhovie.	**Výsledok:** Sťažnosť proti odstráneniu obsahu **nie je opodstatnená**, a preto sa zamieta.
Význam: Obsah bol nesprávne odstránený, vymazaný alebo inak moderovaný.	**Význam:** Obsah bol správne odstránený, vymazaný alebo inak moderovaný.
Ďalší postup: HSP (1) informuje sťažovateľa o výsledku preskúmania a (2) obnoví obsah.	**Ďalší postup:** HSP (1) informuje sťažovateľa o výsledku preskúmania a (2) poskytne používateľovi dôvody tohto rozhodnutia.

4. Praktické tipy a rady: Aké prvky sú užitočné pri vytváraní systému podávania sťažností?

To, že systém podávania sťažností musí mať určité funkcie, nie je len požiadavka zákona, ale aj požiadavka **používateľskej prívetivosti**.

Podobne ako iné kľúčové otázky, ako sú ToS (▶kapitola 1), zavedenie procesu identifikácie zakázaného obsahu (▶kapitola 2), alebo výber moderovacích mechanizmov špecifických pre platformu (▶kapitola 3), aj spôsob podávania sťažností sa môže medzi platformami značne líšiť. Zatiaľ čo niektoré platformy môžu ponúkať podávanie sťažností prostredníctvom e-mailu, iné sa rozhodnú zaviesť štandardizované online aplikácie založené na formulároch. **Systémy podávania sťažností by mali byť prispôsobené účelu, štruktúre a organizácii platformy**. Usmernenia k vytvoreniu systému sťažností nájdete v nasledujúcom **kontrolnom zozname.**

Uveďte jasné informácie o odstránení obsahu

Upozornite osobu, ktorej obsah bol odstránený. Zvážte tento postup aj v prípade, že bol obsah moderovaný iným spôsobom. V tejto súvislosti informujte osobu aj o tom, prečo bol obsah odstránený (pozri nasledujúci bod o výchovných a pedagogických súvislostiach) a ako sa možno proti rozhodnutiu o odstránení odvolať (pozri nasledujúci bod o vysvetlení procesu podávania sťažností).

Vysvetlite postup podávania sťažností

Vysvetlite používateľom postup podávania sťažností. Malo by sa tak stať v rámci oznámenia o odstránení obsahu alebo jeho inej moderácii. Informácie o postupe podávania sťažností môžete uviesť aj v ToS. Vysvetlenie procesu podávania sťažností by

malo obsahovať: (1) ako možno podávať sťažnosti, (2) ako funguje proces preskúmania a (3) ako sú používatelia informovaní o výsledku preskúmania.

Poskytnúť základné pedagogické informácie

Poskytnite používateľom vzdelávacie príležitosti, aby ste vysvetlili, prečo bol obsah odstránený a ktoré podmienky porušuje. Obsah môže byť napríklad odstránený, ak porušuje ToS alebo ak bola v rámci nariadenia o TCO prijatá žiadosť o odstránenie od príslušného orgánu. V prvom prípade možno túto informáciu spresniť pridaním informácie, ktorý z ToS zákazov špecifických pre platformu bol porušený (napr. proti nenávistným prejavom, podnecovaniu k násiliu, sexuálnemu obsahu a obťažovaniu). V druhom prípade sa odporúča pridať do systému sťažností stručný informatívny prehľad nariadenia o TCO, aby bol používateľovi jasný právny rámec.

Pravidelne informujte o priebehu vybavovania sťažnosti

Používateľom by sa mali pravidelne poskytovať aktuálne informácie o priebehu vybavovania sťažnosti, aby sa preukázalo, že proces pokračuje. Takéto aktualizácie by mali pozostávať minimálne z oznámenia o ukončení preskúmania a včasného oznámenia výsledku. Podrobnejšia komunikácia by mohla používateľovi oznámiť, že sťažnosť bola prijatá a teraz ju zamestnanci HSP preverujú. Osvedčený postup by používateľovi poskytol časový rámec na posúdenie jeho sťažnosti. Tieto aktualizácie sa môžu poskytnúť e-mailom alebo zobraziť na online portáli.

Zdokumentujte (individuálny) proces podávania sťažností

Je dôležité zdokumentovať proces podávania sťažností. Tento dokument bude slúžiť ako referencia pre prípadné následné otázky alebo spory.

Kapitola 6

Praktická podpora a poradenstvo v oblasti podávania správ o transparentnosti

Zhrnutie: Obsah a hlavné body tejto kapitoly

- Správy o transparentnosti umožňujú HSP **verejne informovať** o tom, ako sa na platforme dodržiavajú ich **hodnoty**, a tiež o **opatreniach prijatých proti zakázanému a nelegálnemu obsahu a správaniu**.
- Správy o transparentnosti sú **dôležitým nástrojom na prevzatie verejnej zodpovednosti a preukázanie dôveryhodnosti a spoľahlivosti**.
- Rôzne **právne predpisy** vrátane nariadenia o TCO **výslovne vyžadujú podávanie správ o transparentnosti**.
- Pri príprave správ o transparentnosti sa odporúča postupovať systematicky pred, počas a po procese podľa konkrétnych krokov.
- V **nariadení o TCO sa vyžaduje, aby HSP, ktoré sú vystavené teroristickému obsahu alebo prijali opatrenia proti nemu, zverejnili výročnú správu o transparentnosti svojich činností v súvislosti s teroristickým obsahom**. Správa musí obsahovať určité základné údaje a informácie, ako napríklad počet odstránených obsahov. Správa sa musí uverejniť najneskôr do 1. marca nasledujúceho roka (nariadenie o TCO, článok 7.2).

1. Čo sú to správy o transparentnosti?

Správy o transparentnosti sú **pre HSP dôležitým nástrojom na preukázanie ich zodpovednosti, dôveryhodnosti a spoľahlivosti a na zverejňovanie spoločensky relevantných informácií**. Správy o transparentnosti **obsahujú dôležité údaje o žiadostiach, ktoré HSP dostávajú od štátnych subjektov na celom svete, a o tom, ako sa tieto žiadosti vybavujú**, čo má za cieľ sprehľadniť spoluprácu a kooperáciu s úradmi a inými štátnymi orgánmi[6].

Správy o transparentnosti poskytujú aj prehľad o tom, aké opatrenia HSP prijali na presadzovanie predpisov (napr. prostredníctvom odstraňovania obsahu alebo iných moderátorských opatrení). Patrí sem presadzovanie (1) zásad špecifických pre platformu (zvyčajne ToS; ▶kapitola 1), (2) práv, ako sú autorské práva alebo zákon o ochranných známkach, a (3) (miestnych) právnych predpisov a nariadení, ktoré vedú k odstráneniu obsahu. V EÚ medzi miestne právne predpisy patrí nariadenie o TCO a DSA. Relevantné môžu byť aj právne predpisy špecifické pre jednotlivé krajiny, ako napríklad zákon o presadzovaní sieťových práv v Nemecku.

[6] Urman, A., & Makhortykh, M. (2023). How transparent are transparency reports? Comparative analysis of transparency reporting across online platforms. *Telecommunications Policy, 47*(3), 102477. https://doi.org/10.1016/j.telpol.2022.102477

Správy o transparentnosti sa zvyčajne zverejňujú pravidelne. V nariadení o TCO sa uvádza, že by sa to malo robiť **(aspoň) raz ročne**, ak HSP prijal opatrenia proti teroristickému obsahu (nariadenie o TCO, 30).

Správy o transparentnosti a v nich uvádzané ukazovatele sa môžu značne líšiť od jedného HSP k druhému[7]. **V prípade správ o transparentnosti v súlade s nariadením o TCO existujú osobitné požiadavky na to, aké informácie musia byť zahrnuté.** Viac informácií nájdete v ▶odstavci 4 tejto kapitoly.

2. Prečo sú správy o transparentnosti potrebné?

Správy o transparentnosti **umožňujú používateľom a tretím stranám posúdiť, do akej miery HSP dodržiavajú svoje vlastné zásady, právne požiadavky a ochranu údajov a súkromia**[9]. Pozrime sa na rôzne pohľady na to, prečo sú správy o transparentnosti dôležité.

a) Právne hľadisko

Správy o transparentnosti sú užitočné a často potrebné na dodržiavanie nariadení EÚ, ako je nariadenie o TCO, DSA a prípadne zákony jednotlivých krajín. Ak HSP prijali opatrenia proti šíreniu teroristického obsahu v priebehu kalendárneho roka, či už proaktívne alebo v súlade s príkazom na odstránenie, správa o transparentnosti sa **musí uverejniť najneskôr do 1. marca nasledujúceho roka** (nariadenie o TCO, článok 7.2). To znamená, že správy o transparentnosti budú s vyššou pravdepodobnosťou povinné. Príslušné orgány sú tiež povinné uverejňovať výročné správy o transparentnosti (nariadenie o TCO, 31).

b) Hľadisko používateľa a zainteresovaných strán

Správy o transparentnosti pomáhajú používateľom a ďalším zainteresovaným stranám posúdiť, do akej miery si HSP plnia svoju **zodpovednosť voči spoločnosti**. Pravidelné zverejňovanie správ o transparentnosti zároveň pomáha HSP **budovať dôveru a dobrú verejnú reputáciu** tým, že preukazuje dodržiavanie predpisov, angažovanosť a spoľahlivosť.

c) Hľadisko spoločnosti

Podobne ako mechanizmy podávania sťažností, aj správy o transparentnosti môžu byť **nástrojom samokontroly**, ktorý identifikuje oblasti, v ktorých je možné optimalizovať podnikové procesy. Vzhľadom na to, že menšie HSP sú obzvlášť obľúbené u teroristických aktérov (podrobnosti nájdete v tejto správe Tech Against Terorism), je ich povinnosťou prijať opatrenia proti šíreniu teroristického obsahu. Správy o transparentnosti sú jedným zo spôsobov, ako môžu menší HSP preukázať svoju angažovanosť v tomto úsilí.

[7] Woolery, L., Budish, R., & Bankston, K. (2016). The transparency reporting toolkit. *New America and The Berkman Center for Internet & Society at Harvard University*.

3. Proces prípravy správ o transparentnosti

Úvodné nastavenie a predloženie správy o transparentnosti môže byť náročnou úlohou. Po zavedení **procesu a rutiny prípravy výročných správ o transparentnosti** však zvyčajne nie je potrebné úplne prepracovať štruktúru správy a zvyčajne postačí jej aktualizácia. V tejto príručke sa uvádza, ako nastaviť správu o transparentnosti z pohľadu HSP, ako aj to, čo treba zvážiť pred, počas a po procese tvorby.

a) **Pred** vypracovaním správy o transparentnosti

Preskúmajte právne prostredie

Zoznámte sa s právnymi predpismi, ktoré sa vzťahujú na vaše HSP. Napríklad nariadenie o TCO a DSA sú relevantné v celej EÚ. Môžu existovať predpisy špecifické pre jednotlivé krajiny, ako aj požiadavky na ďalšie záležitosti relevantné pre váš HSP mimo teroristického obsahu. Ak ste v kontakte s právnikmi, je vhodné vymeniť si s nimi informácie, aby ste zistili, ktoré ďalšie predpisy (okrem nariadenia o TCO) sa na vás vzťahujú.

Určite ciele správy o transparentnosti

Premyslite si, aké sú ciele vašej správy o transparentnosti. Kľúčové otázky, ktoré vám pri tom môžu pomôcť, sú: Chcete jednoducho "len" splniť svoje zákonné povinnosti, alebo sa chcete venovať aj iným témam a svojim záväzkom voči nim? Koho chcete osloviť, t. j. ktorá cieľová skupina má pre vás zmysel (napr. politické subjekty, používatelia, finančníci)? Ako často chcete zverejňovať správy o transparentnosti a aký je najvhodnejší čas pre váš individuálny finančný rok?

Určite, ktoré údaje sa môžu a majú zahrnúť

Určite, ktoré údaje zahrniete do správy o transparentnosti. Na jednej strane je pre to relevantná *schopnosť*, t. j. aké údaje sú k dispozícii alebo v prípade ktorých je reálne, že ich môžete v budúcnosti zhromaždiť? Na druhej strane je rozhodujúca *povinnosť*, t. j.: aké právne požiadavky musíte splniť a aké údaje sú na to potrebné? Aké informácie a údaje musíte uviesť v súlade s nariadením o TCO, sa dozviete v ▶ v ďalšej podkapitole.

b) **Počas** tvorby správy o transparentnosti

Používajte jasný a stručný jazyk

Pri tvorbe správy o transparentnosti dbajte na to, aby ste používali jasný a stručný jazyk. Pomáha to pri zaujatí a pochopení zložitého a komplexného materiálu. Jazyk by sa mal ďalej prispôsobiť predpokladanej skupine čitateľov.

Poskytnúť kontextové informácie a vysvetlenia

Poskytnite čitateľom informácie a vysvetlenia v súvislostiach. Takéto vysvetlenia umožnia používateľom lepšie pochopiť spôsob, akým váš HSP funguje, a dôvody, prečo (možno) poskytuje podrobnejšiu správu o transparentnosti ako "len" správu spĺňajúcu len minimálne regulačné požiadavky.

Zapracujte internú spätnú väzbu

Pri plánovaní správy o transparentnosti zahrňte do časového harmonogramu výroby aj jednotlivé fázy spätnej väzby. Pravidelná spätná väzba umožňujúca korekcie obsahu a jazyka správy môže byť cenná pre všetkých zúčastnených aktérov, najmä pre tých, ktorí sú poverení prípravou správy.

c) **Po** vypracovaní správy o transparentnosti

Uverejnite správu o transparentnosti

Zvážte, v ktorých jazykoch chcete správu o transparentnosti zverejniť, a vytvorte príslušné preklady. Stanovte tiež, kde by mala byť prístupná, t. j. na vašej webovej stránke. Okrem toho môžete zvážiť aj zaradenie správy o transparentnosti do rôznych komunikačných materiálov, aby ste jej pomohli získať väčšiu pozornosť. Môže to zahŕňať jej vloženie na vašu webovú stránku, rozposlanie v e-mailových bulletinoch alebo zdieľanie na sociálnych sieťach.

Pravidelne aktualizujte údaje a napokon aj správu o transparentnosti

Po dokončení prvej správy o transparentnosti už máte vybudovaný základ, ktorý vám uľahčí nasledujúcu správu vzhľadom na to, že ste už vytvorili šablónu. Proces zhromažďovania príslušných údajov počas celého roka a ich usporiadanie tak, aby boli ľahko vyhľadateľné, uľahčí vypracovanie ďalšej správy o transparentnosti a bude menej náročný na čas a zdroje.

Poskytnite priestor na zlepšenie

Buďte otvorení zmenám a úpravám. Ak dostanete externú spätnú väzbu, zvážte jej zapracovanie do ďalšej správy o transparentnosti, ak je to vhodné. Relevantná spätná väzba však nemusí byť len externá. Po zverejnení správy o transparentnosti sa HSP môže kriticky pozrieť aj na predchádzajúcu správu o transparentnosti, komunikáciu okolo nej a reakcie na ňu, a to tak, že zváži vyjadrenia v tlači alebo iné relevantné zdroje. Interná aj externá spätná väzba môže určiť, kde môže byť priestor na zlepšenie.

4. Aké informácie a ukazovatele je potrebné zahrnúť do správy o transparentnosti?

V článku 7.3 nariadenia o TCO sa vysvetľujú minimálne požiadavky na správy o transparentnosti, t. j. čo presne je potrebné uviesť, aby boli v súlade s týmto právom EÚ. Tieto požiadavky uvádzame v kontrolnom zozname nižšie:

1) **Informácie** o tom, aké opatrenia HSP prijal:
- ☑ na identifikáciu teroristického obsahu;
- ☑ na odstránenie alebo zakázanie teroristického obsahu;
- ☑ aby sa zabránilo opätovnému výskytu a nahrávaniu už zablokovaných online materiálov (to je dôležité najmä v prípade, že sa používajú automatizované postupy).

2) **Metriky** a prípadne ďalšie informácie týkajúce sa počtu:
- ☑ odstránených položiek, ktoré obsahujú teroristický obsah (na základe príkazov na odstránenie alebo iných opatrení);
- ☑ príkazov na odstránenie, ktoré neboli vykonané, a doplňujúce informácie o tom, prečo sa tak nestalo;
- ☑ sťažnosti, ktoré HSP vybavil prostredníctvom mechanizmu podávania sťažností, ako aj doplňujúce informácie o výsledku sťažností;
- ☑ prípady, v ktorých HSP obnovil obsah na základe sťažnosti poskytovateľa obsahu;
- ☑ právne konania, ktoré inicioval HSP, a doplňujúce informácie o výsledku týchto konaní;
- ☑ prípady, v ktorých HSP musel obnoviť obsah po právnom konaní.

C. Ďakujeme vám za pomoc v boji proti hrozbe terorizmu!

Gratulujeme!

Dostali ste sa až sem, a to znamená, že ste získali základné vedomosti o požiadavkách nariadenia o TCO a ďalších opatreniach na boj proti teroristickému a inému škodlivému obsahu na internete. Týmto spôsobom prispejete k bezpečnejšiemu internetu.

Sme si vedomí, že implementácia týchto opatrení si vyžaduje značnú pozornosť a zdroje. Skutočnosť, že ste sa zaoberali touto príručkou, je skvelým krokom. Ak vám táto príručka pomôže premyslieť stratégiu zavádzania opatrení proti teroristickému obsahu, ktorá je pre vás vhodná, považujeme to za veľký úspech! Sme presvedčení, že táto príručka, spolu s našimi ďalšími vzdelávacími materiálmi, bude pre vás cenným nástrojom, umožňujúcim v plnej miere plniť povinnosti v oblasti boja proti teroristickej hrozbe online.

Ďakujeme vám za váš záujem bojovať proti teroristickej hrozbe online a za to, že sa snažíte brániť služby HSP a svojich používateľov.

PS: Súčasťou projektu Tech Against Terrorism Europe je aj **bezplatný a ocenený online kurz**, v ktorom sa môžete bližšie oboznámiť s dodržiavaním nariadenia o TCO. V tomto kurze sa môžete ponoriť hlbšie do problematiky a nájsť podrobnosti o nariadení, príklady implementácie jednotlivých opatrení inými platformami a všeobecnejšie informácie o teroristickom správaní online. **Po úspešnom absolvovaní kurzu získate oficiálny certifikát podpísaný renomovanými univerzitami** (LMU Mníchov, Univerzita v Gente). Okrem toho TATE ponúka Program budovania kapacít, v rámci ktorého môžu HSP získať praktickú podporu pri plnení požiadaviek súvisiacich s nariadením o TCO.

D. Slovník

Pojem	Vysvetlenie
Ppríslušné orgány	Orgány členského štátu EÚ, ktoré sú zodpovedné za vykonávanie nariadenia o TCO. Prehľad príslušných orgánov členských štátov nájdete tu.
Poskytovateľ obsahu	Osoba, ktorá poskytuje obsah na príslušnej platforme, napríklad publikuje príspevok.
HSP	Poskytovatelia hostingových služieb; nariadenie o TCO sa vzťahuje na HSP. Podrobnejšie informácie o tom, na ktorých HSP sa vzťahuje nariadenie o TCO, nájdete tu (B).
PERCI	PERCI je nástroj koordinovaný Europolom, ktorý je určený na zlepšenie a uľahčenie komunikácie medzi HSP a príslušnými orgánmi.
Príkaz na odstránenie	Žiadosť, ktorú HSP dostane od príslušného orgánu. Informuje HSP o tom, že na platforme bol šírený teroristický obsah, a zaväzuje HSP, aby ho do jednej hodiny od prijatia urýchlene odstránil.
Nariadenie o TCO (tiež: LEX 2021/784 a Nariadenie o riešení šírenia teroristického obsahu online)	Nariadenie EÚ o riešení šírenia teroristického obsahu online, ktoré nadobudlo účinnosť v roku 2022. Vzťahuje sa na poskytovateľov hostingových služieb (HSP), ktorí ponúkajú svoje služby v EÚ.
Teroristický obsah online (TCO)	Obsah, ktorý obsahuje teroristické prvky alebo má za cieľ propagovať teroristické účely. Podrobnú definíciu nájdete v ▶úvode. Teroristický obsah na internete úzko súvisí s ▶teroristickými trestnými činmi, ktoré môžu mať veľmi rôznorodý charakter.
ToS	Podmienky užívania (Terms of Service); Záväzné pravidlá stanovené jednotlivými platformami a pre jednotlivé platformy, ktoré (1) vymedzujú rozsah a zodpovednosť HSP voči používateľom a (2) vhodné a povolené, ale aj zakázané postupy používania. Používatelia ich musia dodržiavať, ak chcú naďalej využívať služby ponúkané HSP. Existuje množstvo synoným pre ToS, napr. podmienky používania, zmluvné podmienky alebo štandardy komunity