EUROPEAN BOARD FOR DIGITAL SERVICES

Oznamovanie podozrení z trestných činov podľa článku 18 DSA

Osvedčené postupy

Október 2026

Vyhlásenie

Preložený dokument je výsledkom aktivít pracovnej skupiny č. 7 – Príkazy a trestnoprávne otázky Európskeho výboru pre digitálne služby („Výbor“). Slúži výlučne ako praktický referenčný zdroj, nie je právne záväzný a neprejudikuje žiadne budúce stanovisko Komisie, výboru, koordinátorov digitálnych služieb a iných orgánov členských štátov. Týmto dokumentom nie je dotknutý výklad nariadenia (EÚ) 2022/2065 (DSA) Súdnym dvorom Európskej únie.

1. ÚVOD 5
2. ROZSAH 6
3. POJEM „POVEDOMIE“ 7
3.1 Zdroje informácií 7
3.2 Dôsledné posúdenie 9
4. TRESTNÉ ČINY, KTORÝCH DÔSLEDKOM BÝVA OHROZENIE ŽIVOTA ALEBO BEZPEČNOSTI 10
4.1 Národné prílohy 11
4.2 Oznámenia týkajúce sa samovraždy a/alebo sebapoškodzovania 11
5. PRAKTICKÉ PRÍKLADY INDIKÁTOROV 12
6. URČENIE DOTKNUTÉHO ČLENSKÉHO ŠTÁTU 16
6.1 Postup interného posudzovania 16
6.2 Oznámenia, ktoré sa týkajú viacerých členských štátov 17
6.3 Oznámenia, pri ktorých nie je možné s primeranou istotou identifikovať dotknutý členský štát 17
7. POSKYTOVANIE RELEVANTNÝCH INFORMÁCIÍ 18
8. OZNAMOVACIE A KOMUNIKAČNÉ KANÁLY 20
8.1 Jednotné kontaktné miesta (SPOC) 20
8.2 Technické riešenia pre poskytovanie informácií 21
8.3 Interakcia s inými oznamovacími povinnosťami 21
9. DOHLAD NAD DODRŽIAVANÍM PREDPISOV 22
10. PREHĽAD DOKUMENTU 23

1. ÚVOD

Článok 18 ods. 1 aktu o digitálnych službách (**DSA**)[1] vyžaduje, aby poskytovatelia hostingových služieb (ďalej len „**poskytovatelia**“) bezodkladne informovali orgány presadzovania práva alebo justičné orgány (ďalej spoločne len „**orgány**“) príslušného členského štátu alebo príslušných členských štátov, ak sa dozvedia o akýchkoľvek informáciách, ktoré vedú k podozreniu, že došlo k trestnému činu, ktorého dôsledkom je ohrozenie života alebo bezpečnosti osoby alebo osôb, dochádza k nemu alebo je pravdepodobné, že k nemu dôjde. Pri oznamovaní orgánom poskytovatelia poskytujú všetky dostupné relevantné informácie.

Článok 18 ods. 2 DSA uvádza, že dotknutým členským štátom je ten členský štát, v ktorom existuje podozrenie, že došlo k trestnému činu, že k nemu dochádza alebo pravdepodobne dôjde, alebo členský štát, v ktorom má podozrivý zo spáchania trestného činu pobyt alebo sa v ňom nachádza, alebo členský štát, v ktorom má pobyt alebo sa nachádza obeť údajného trestného činu. Ak poskytovatelia digitálnych služieb nemôžu s primeranou istotou identifikovať dotknutý členský štát, informujú členský štát, v ktorom majú sídlo alebo právne zastúpenie, alebo informujú Europol, alebo oboch.

Európsky výbor pre digitálne služby (ďalej len „**výbor**“) pripomína, že poskytovatelia digitálnych služieb sa môžu dostať do situácie, keď sa dozvedia o informáciách, ktoré sú kľúčovou podmienkou pre orgány, aby mohli následne vyšetrovať trestné činy a zabrániť naplneniu hrozby voči životu alebo bezpečnosti osoby. Takéto ohrozenie nemusí byť namierené proti jednej alebo viacerým identifikovateľným osobám, ale môže sa týkať širokej verejnosti. Výbor preto opätovne zdôrazňuje význam článku 18 DSA v situáciách, ktoré predstavujú ohrozenie života alebo bezpečnosti širokej verejnosti, a to vrátane prípadov, keď trestný čin môže vyvolať verejnú krízu, a so zreteľom na nebezpečné alebo život ohrozujúce online výzvy, ktoré nabádajú alebo priamo inštruujú používateľov k páchaniu trestných činov.

Výbor na základe konzultácií s koordinátormi digitálnych služieb (ďalej len „**koordinátormi**“) a so zástupcami orgánov konštatuje, že od úplného nadobudnutia účinnosti DSA dňa 17. februára 2024 viaceré členské štáty nedostali žiadne alebo dostali len veľmi málo oznámení podľa článku 18 DSA. Niektorí poskytovatelia zasielajú oznámenia v prvom rade iba Europolu, prípadne nesprávnemu členskému štátu, hoci by bolo možné s primeranou istotou identifikovať príslušný členský štát. To môže viesť k oneskoreniam pri oznamovaní orgánom a negatívne sa prejaviť najmä v prípadoch bezprostredného alebo pretrvávajúceho ohrozenia života alebo bezpečnosti. Okrem toho výbor v súvislosti s oznámeniami prijatými od poskytovateľov konštatuje výrazné rozdiely v počte oznámení, rozsahu oznámených trestných činov a relevantnosti predložených informácií, pričom tieto prvky sú z hľadiska opatrení orgánov kľúčové. Výbor okrem toho konštatuje, že hoci majú koordinátori za úlohu v rámci svojej jurisdikcie dohliadať na dodržiavanie článku 18 DSA, často nemajú k dispozícii informácie o oznámeniach zasielaných poskytovateľmi orgánom, čo predstavuje významné prekážky pri presadzovaní tohto článku.

Vzhľadom na vyššie uvedené skutočnosti výbor konštatuje nejednotnosť pri uplatňovaní článku 18 DSA zo strany poskytovateľov a zastáva názor, že vytvorenie uceleného prehľadu osvedčených postupov a praktických príkladov prispeje k zlepšeniu spoločného chápania povinností stanovených v tomto článku.

Výbor pripomína, že podľa recitálu č. 9 DSA je kľúčovým cieľom DSA zaistiť bezpečné, predvídateľné a dôveryhodné online prostredie, v ktorom sú účinne chránené základné práva zakotvené v Charte základných práv Európskej únie. Ako sa uvádza najmä v recitáli č. 56, poskytovatelia hostingových služieb by mali dodržiavať uplatniteľné pravidlá práva Únie alebo vnútroštátneho práva na ochranu práv a slobôd fyzických osôb, vrátane práv obetí. Pri uplatňovaní článku 18 by sa preto mali tieto práva a slobody plne rešpektovať.

(1) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES.

2. ROZSAH

Tento dokument má slúžiť ako praktický zdroj informácií a podporovať jednotné uplatňovanie DSA vo všetkých členských štátoch v súlade s článkom 61 ods. 2 písm. a) DSA tým, že poskytne ucelený prehľad osvedčených postupov a praktických príkladov a pomôže tak koordinátorom aj Komisii pri dohľade nad dodržiavaním článku 18 DSA. Cieľom je tiež prispieť k zabezpečeniu toho, aby poskytovatelia náležite a bezodkladne informovali príslušné orgány v dotknutých členských štátoch a poskytovali im všetky relevantné informácie, ktoré majú k dispozícii.

Dokument je výsledkom spoločného úsilia v rámci pracovnej skupiny č. 7 výboru. Náležite zohľadňuje výsledky cielených konzultácií pod vedením Komisie v období od 18. novembra 2025 do 9. januára 2026. V rámci týchto konzultácií boli zozbierané pripomienky príslušných zainteresovaných strán, vrátane orgánov presadzovania práva a justičných orgánov, poskytovateľov hostingových služieb, podnikateľských združení a mimovládnych organizácií, týkajúce sa oblastí vyžadujúcich ďalšie objasnenie, ako aj osvedčených postupov a praktických príkladov v súvislosti s uplatňovaním článku 18 DSA.[(2)]

Výsledkom je dokument s nasledujúcimi tematickými časťami:

- vysvetlenie pojmu „povedomie“ vrátane prehľadu zdrojov relevantných informácií (časť 3);
- prehľad trestných činov (nie konečný), ktorých dôsledkom je zvyčajne ohrozenie života alebo bezpečnosti (časť 4);
- praktické príklady indikátorov vedúcich k podozreniu z trestných činov, ktorých dôsledkom je ohrozenie života alebo bezpečnosti (časť 5);
- osvedčené postupy identifikácie dotknutého členského štátu alebo štátov (časť 6);
- osvedčené postupy poskytovania relevantných informácií poskytovateľmi orgánom (časť 7);
- príklady oznamovacích a komunikačných kanálov na podávanie oznámení orgánom (časť 8);
- aspekty dohľadu nad dodržiavaním článku 18 DSA (časť 9).

Hoci praktické príklady vychádzajú zo skutočných udalostí a prípadov, všetky mená uvedené v tomto dokumente sú fiktívne.

(2) Súhrnná správa o výsledkoch cielených konzultácií týkajúcich sa oznamovania podozrení z trestných činov podľa DSA je k dispozícii tu: https://digital-strategy.ec.europa.eu/en/library/factual-summary-report-targeted-consultation-notification-suspicions-criminal-offences-under-dsa.

3. POJEM „POVEDOMIE“

Povinnosť poskytovateľov hostingových služieb informovať orgány presadzovania práva a justičné orgány vzniká v okamihu, keď sa dozvedia o informáciách, ktoré vedú k podozreniu z trestného činu, ktorého dôsledkom je ohrozenie života alebo bezpečnosti.

Výbor pripomína, že ak sa poskytovatelia po zistení určitého obsahu rozhodnú tento obsah odstrániť alebo k nemu zablokovať prístup (napr. preto, že ide o nezákonný obsah alebo porušuje ich obchodné podmienky), nemá to vplyv na ich povinnosť oznámiť to príslušnému orgánu podľa článku 18 DSA, ak je to relevantné. To zahŕňa aj povinnosť poskytnúť dostupné relevantné informácie.

3.1 Zdroje informácií

Na základe získanej spätnej väzby, najmä výsledkov cielených konzultácií a výmeny názorov v pracovnej skupine č. 7, výbor konštatuje, že poskytovatelia sa môžu dozvedieť o relevantných informáciách zmysle článku 18 DSA z rôznych zdrojov, a to vrátane oznámení používateľov, oznámení od dôveryhodných nahlasovateľov a dobrovoľných mechanizmov, ako aj na základe monitorovania a vyšetrovania z vlastnej iniciatívy. Prehľad týchto zdrojov, ako aj príklady osvedčených postupov, sú uvedené nižšie.

Povedomie na základe oznámení používateľov

Podľa článku 16 ods. 1 DSA sú poskytovatelia hostingových služieb povinní zaviesť mechanizmy oznamovania a prijímania opatrení, ktoré každému jednotlivcovi alebo subjektu umožnia oznámiť im prítomnosť konkrétnych informácií, ktoré tento jednotlivec alebo subjekt považuje za nezákonný obsah v ich službe. V závislosti od typu služby, jej rozsahu a dostupných zdrojov môže poskytovateľ disponovať aj ďalšími mechanizmami podávania oznámení v súlade s inými povinnosťami vyplývajúcimi z práva Únie alebo práva členského štátu v súlade s právom Únie, ako aj mechanizmami, ktoré používateľom umožňujú oznamovať podozrenia z porušenia podmienok používania služby.

Takéto oznámenia a hlásenia používateľov sa môžu týkať informácií, ktoré buď samy osebe, alebo v kombinácii s odôvodnením, prečo jednotlivec alebo subjekt tvrdí, že dané informácie sú nezákonné alebo porušujú obchodné podmienky, naznačujú podozrenie z trestného činu, ktorého dôsledkom je ohrozenie života alebo bezpečnosti.

Osvedčená prax: Oznámenia používateľov

V súlade s povinnosťami článku 16 ods. 1 DSA poskytuje online platforma *ABC Gaming Forum* mechanizmus oznamovania a prijímania opatrení, ktorý umožňuje používateľom oznamovať informácie, ktoré považujú za nezákonný obsah. *ABC Gaming Forum* posudzuje nahlásený obsah so zreteľom na prvky uvedené v článku 16 ods. 2 DSA, najmä či vysvetlenie dôvodov, prečo oznamovateľ považuje obsah za nezákonný, obsahuje relevantné náznaky trestného činu, ktorého dôsledkom je ohrozenie života alebo bezpečnosti. *ABC Gaming Forum* dobrovoľne dopĺňa do tohto mechanizmu možnosť, ktorá používateľom umožňuje označiť, že oznámenie poukazuje na ohrozenie života alebo bezpečnosti, s cieľom uľahčiť poskytovateľovi posudzovanie oznámenia. *ABC Gaming Forum* implementuje túto dobrovoľnú možnosť takým spôsobom, aby neovplyvňovala dostupnosť ani užívateľskú prívetivosť mechanizmu oznamovania a prijímania opatrení.

Povedomie na základe oznámení dôveryhodných nahlasovateľov a dobrovoľných mechanizmov

V súlade s článkom 22 DSA sú poskytovatelia hostingových služieb, ktoré sú online platformami, povinní zabezpečiť, aby oznámenia podané subjektmi, ktorým koordinátor udelili štatút dôveryhodného nahlasovateľa, mali prednosť a spracúvali sa bez zbytočného odkladu. Odbornosť dôveryhodných nahlasovateľov sa týka odhaľovania, identifikácie a oznamovania konkrétnych typov nezákonného obsahu, ako je napríklad obsah súvisiaci so sexuálnym zneužívaním detí, obchodovaním s ľuďmi alebo terorizmom. Od úplného nadobudnutia účinnosti DSA udelili koordinátori v členských štátoch štatút dôveryhodného nahlasovateľa viac než 80 subjektom s rôznorodými odbornými znalosťami. Okrem toho môžu poskytovatelia dobrovoľne spolupracovať s externými odborníkmi, napríklad s organizáciami občianskej spoločnosti, s cieľom riešiť konkrétne typy obsahu, ktoré nie sú v súlade s ich obchodnými podmienkami.

Hoci v zásade môže každé oznámenie obsahovať relevantné informácie, očakáva sa, že oznámenia prijaté od dôveryhodných nahlasovateľov alebo od partnerov v rámci dobrovoľných mechanizmov, ktorí majú odborné znalosti v príslušných oblastiach trestnej činnosti, budú presnejšie. Preto môžu takéto oznámenia mať osobitný význam pri nadobudnutí povedomia o trestných činoch, ktorých dôsledkom je ohrozenie života alebo bezpečnosti.

Povedomie na základe opatrení z vlastnej iniciatívy

Hoci podľa článku 8 DSA sa poskytovateľom hostingových služieb neukladá žiadna všeobecná povinnosť monitorovať prenášané alebo ukladané informácie, ani povinnosť aktívne zisťovať skutočnosti alebo okolnosti naznačujúce nezákonnú činnosť, nebráni to poskytovateľom, aby dobrovoľne a proaktívne vyhľadávali obsah naznačujúci trestný čin, ktorého dôsledkom je ohrozenie života alebo bezpečnosti. Na základe získanej spätnej odozvy možno konštatovať, že niektorí poskytovatelia vykonávajú v rámci svojich služieb dobrovoľné monitorovanie alebo vyšetrovanie z vlastnej iniciatívy, a to aj prostredníctvom automatizovaných systémov a manuálnej ľudskej kontroly s cieľom identifikovať nezákonný obsah alebo obsah porušujúci ich obchodné podmienky. Aj takýto obsah môže vyvolať podozrenie z trestného činu podľa článku 18 DSA.

Osvedčená prax: Opatrenia z vlastnej iniciatívy

Všeobecné obchodné podmienky spoločnosti *ABC Network* výslovne zakazujú určitý typ obsahu, predovšetkým vyhrážky fyzickým násilím, propagáciu alebo glorifikáciu násilia, nenávistné prejavy a nenávistné správanie, sexuálne zneužívanie a vykorisťovanie, ako aj obťažovanie a šikanovanie. Spoločnosť *ABC Network* vo svojej službe využíva systémy moderovania obsahu na presadzovanie svojich obchodných podmienok. Vzhľadom na značný rozsah obsahu, ktorý do služby nahrávajú používatelia, spoločnosť *ABC Network* využíva automatizované detekčné systémy, a to vrátane modelov strojového učenia, ktoré vo veľkej miere pomáhajú odhaľovať obsah porušujúci obchodné podmienky a nezákonný obsah. Detekčné systémy môžu eskalovať obsah s vysokou závažnosťou vo všetkých jazykoch EÚ svojim bezpečnostným tímom, ktorých pracovníci disponujú špecializovanými znalosťami a odbornými znalosťami a vykonávajú ďalšie kontextové, sémantické a jazykové posúdenia.

3.2 Dôsledné posúdenie

Výbor pripomína, že povinnosť stanovená v článku 18 ods. 1 DSA vo všeobecnosti od poskytovateľov hostingových služieb nevyžaduje istotu vedomosti, že došlo, dochádza alebo dôjde k trestnému činu, ktorého dôsledkom je ohrozenie života alebo bezpečnosti – stačí už samotné podozrenie. Potvrdenie takéhoto podozrenia si však vyžaduje dôkladné posúdenie nadobudnutých informácií.

Na základe získanej spätnej odozvy táto časť uvádza príklady opatrení na podporu posudzovania informácií, ktoré poskytovatelia získajú prostredníctvom príslušných zdrojov. Výbor na základe praxe odporúča, aby takéto informácie posudzovali ľudia s odbornými znalosťami a skúsenosťami (napr. v príslušných oblastiach trestnej činnosti), s cieľom potvrdiť podozrenie podľa článku 18 DSA. Ľudský dohľad, odborné znalosti a zodpovednosť znižujú riziko systematického nadmerného alebo nedostatočného oznamovania prípadov príslušným orgánom.

Medzi takéto opatrenia môžu patriť:

- Pravidelné posudzovanie spôsobov, akým konkrétne charakteristiky, povaha a využívanie služby ovplyvňujú kategórie trestných činov, ktoré sa v rámci služieb vyskytujú.

- Vytvorenie súboru interne definovaných kritérií, signálov a prahových hodnôt pre automatizované systémy detekcie a kontroly s cieľom eskalovať podozrenia z ohrozenia života alebo bezpečnosti na posúdenie človekom. Modely strojového učenia sa neustále testujú a overujú, napríklad pomocou špecifikovaných hodnotiacich metrík a pod dohľadom ľudí.

- Vytvorenie a pravidelné aktualizovanie štandardných operačných postupov (SOP), ktoré stanovujú postupy a taktické kroky umožňujúce posúdenie relevantných informácií špecializovaného ľudského dohľadu. Takéto SOP vychádzajú zo súboru interne definovaných kritérií, signálov a prahových hodnôt, pričom zohľadňujú napríklad:
    - dôveryhodnosť a závažnosť podozrenia hrozby, vrátane prítomnosti identifikovateľnej obete (obetí) alebo miesta (miest);
    - históriu príslušných používateľských účtov;
    - jazykové prvky, ako napríklad regionálny slang, kódovaný jazyk alebo žargón v rámci skupiny vo všetkých jazykoch EÚ;
    - estetické prvky, ako sú symboly, znaky a memetický obsah;
    - odborné znalosti osoby, subjektu alebo partnera, ktorý obsah nahlásil, ak je to relevantné;
    - ďalšie kontextové a technické informácie.

- Pravidelné organizovanie interných školení s cieľom zabezpečiť oboznámenie sa tímov s SOP.

- Udržiavanie jednoduchých, jasne definovaných interných postupov triedenia a eskalácie, ktoré umožnia ľudskému dohľadu rýchlo označiť konkrétne situácie, ako sú bezprostredné alebo pretrvávajúce ohrozenia života alebo bezpečnosti príslušnému tímu (tímom) a vedeniu.

- Vymenovanie špeciálne vyškolených pracovníkov ľudského dohľadu so špecializovanými odbornými znalosťami a vedomosťami, ktorí budú zodpovední za vybavovanie oznámení, najmä za konečné posúdenie obsahu a výber relevantných informácií, ktoré zahrnú do oznámenia odoslaného orgánom.

Výbor konštatuje, že zoznam týchto opatrení nie je konečný a môže sa líšiť v závislosti od typu služby, veľkosti a zdrojov, ktorými poskytovateľ disponuje.

4. TRESTNÉ ČINY, KTORÝCH DÔSLEDKOM BÝVA OHROZENIE ŽIVOTA ALEBO BEZPEČNOSTI

Existujú určité typy trestných činov, ktorých dôsledkom je **zvyčajne** ohrozenie života alebo bezpečnosti osoby alebo osôb. Výbor zdôrazňuje, že takéto trestné činy zahŕňajú jednak trestné činy spojené s ohrozením života alebo bezpečnosti jednotlivých osôb, a jednak trestné činy, ktoré predstavujú ohrozenie života a bezpečnosti širokej verejnosti.

Na základe získanej spätnej odozvy táto časť obsahuje všeobecný a nie úplný zoznam kategórií takýchto trestných činov, vrátane tých, ktoré sú harmonizované na úrovni EÚ a podliehajú implementácii do trestného práva príslušného členského štátu:

- Trestné činy proti životu a/alebo telesnej integrite osoby, ako napríklad:
  - úkladná vražda;
  - zabitie a usmrtenie;
  - ublíženie na zdraví;
  - mučenie;
  - trestné činy súvisiace s nezákonným obchodovaním s ľudskými orgánmi a tkanivami.

- Trestné činy proti slobode a ľudskej dôstojnosti, ako napríklad:
  - obchodovanie s ľuďmi[3] vrátane trestných činov týkajúcich sa vykorisťovania na účel prostitúcie alebo inej formy sexuálneho vykorisťovania, nútenej práce alebo služieb, vykorisťovania v rámci trestnej činnosti, neoprávneného odoberania orgánov a vykorisťovania v súvislosti s náhradným materstvom, nútenými sobášmi alebo nezákonnou adopciou;
  - únos a branie rukojemníkov;
  - vydieranie s priťažujúcimi okolnosťami.

- Trestné činy proti sexuálnej integrite a/alebo sebaurčeniu osoby, ako napríklad:
  - sexuálne zneužívanie a sexuálne vykorisťovanie detí[4] vrátane šírenia materiálu zobrazujúceho sexuálne zneužívanie detí, navádzania detí na sexuálne účely a sexuálneho vydierania;
  - násilie páchané na ženách a domáce násilie[5] vrátane mrzačenia ženských pohlavných orgánov, nútených sobášov, zverejňovania intímneho alebo manipulovaného materiálu bez súhlasu dotknutej osoby, kyberšikanovania, kyberobťažovania a podnecovania k násiliu alebo nenávisti prostredníctvom internetu;
  - znásilnenie a sexuálne násilie.

(3) Bližšie špecifikované v smernici Európskeho parlamentu a Rady 2011/36/EÚ z 5. apríla 2011 o prevencii obchodovania s ľuďmi a boji proti nemu a o ochrane obetí obchodovania, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/629/SVV (Ú. v. EÚ L 101, 15.4.2011, s. 1) a ktorou sa mení smernica Európskeho parlamentu a Rady (EÚ) 2024/1712 z 13. júna 2024.

(4) Bližšie špecifikované v smernici Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa mení rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 17.12.2011, s. 1–14) a jej (chystanej) novelizácii.

(5) Bližšie špecifikované v smernici Európskeho parlamentu a Rady (EÚ) 2024/1385 zo 14. mája 2024 o boji proti násiliu na ženách a domácemu násiliu (Ú. v. EÚ L, 2024/1385, 24.5.2024).

- Trestné činy terorizmu, trestné činy proti ľudskosti a/alebo verejnej bezpečnosti, ako napríklad:
  - terorizmus[6] vrátane teroristických trestných činov a trestných činov súvisiacich s teroristickou skupinou, trestných činov súvisiacich s teroristickou činnosťou a teroristickým obsahom online[7];
  - verejné podnecovanie k násiliu alebo nenávisti, namierené proti osobe alebo skupine osôb alebo členovi takejto skupiny definovanej na základe chránených charakteristík;
  - podpaľačstvo, ktorého dôsledkom je smrť alebo zranenie osôb.

- Okrem toho môžu určité druhy všeobecne nebezpečných trestných činov, trestných činov proti verejnej bezpečnosti a/alebo proti životnému prostrediu predstavovať ohrozenie života alebo bezpečnosti osoby alebo osôb, v závislosti od konkrétnej situácie:
  - trestné činy súvisiace s drogami, novými psychoaktívnymi látkami alebo prekurzormi;
  - trestné činy súvisiace so zbraňami, strelnými zbraňami, ich časťami a komponentmi, strelivom, výbušninami a ich prekurzormi;
  - trestné činy súvisiace s napomáhaním neoprávnenému vstupu, tranzitu alebo pobytu[8];
  - trestné činy súvisiace s jadrovými materiálmi alebo inými vysoko rizikovými rádioaktívnymi látkami;
  - trestné činy súvisiace s nebezpečným odpadom;
  - trestné činy súvisiace s nebezpečným narušením cestnej, železničnej, lodnej a leteckej dopravy.

4.1 Vnútroštátne úpravy

Na základe získanej spätnej odozvy výbor konštatuje, že vnútroštátne trestné právo členských štátov môže špecifikovať ďalšie trestné činy v rámci alebo mimo vyššie uvedených kategórií, ktorých dôsledkom je ohrozenie života alebo bezpečnosti a ktoré preto podliehajú povinnostiam podľa článku 18 DSA. Ak sú v členskom štáte k dispozícii vnútroštátne úpravy, v ktorých sú uvedené dodatočné alebo podrobnejšie špecifikované trestné činy, ktoré by sa mali zohľadňovať v príslušnej jurisdikcii, výbor odporúča, aby koordinátori zvážili ich verejné oznámenie, napríklad zverejnením týchto úprav na svojej webovej stránke alebo inými vhodnými prostriedkami.

4.2 Oznámenia týkajúce sa samovraždy a/alebo sebapoškodzovania

Zo získanej spätnej väzby vyplýva, že hoci samovražda a/alebo sebapoškodzovanie samy osebe v zásade nepredstavujú trestný čin podľa práva Únie ani vnútroštátneho práva, prípady, v ktorých existuje podozrenie, že samovražda a/alebo sebapoškodzovanie súvisia s trestným konaním, ako je podnecovanie, nátlak, sexuálne vydieranie alebo grooming, sa považujú za prípady, na ktoré sa vzťahuje povinnosť podľa článku 18 DSA. Vzhľadom na závažnosť hrozby výbor považuje za osvedčenú prax, aby poskytovatelia v prípade pochybností aj naďalej zasielali oznámenia príslušným orgánom. Aj keď obsah súvisiaci so samovraždou a/alebo sebapoškodzovaním nenaznačuje trestný čin, môže byť potrebné takýto obsah nahlásiť podľa vnútroštátnych právnych predpisov o bezpečnosti na internete a/alebo prostredníctvom iných dobrovoľných kanálov na urýchlené hlásenie takýchto hrozieb voči životu alebo bezpečnosti osoby.

(6) Bližšie špecifikované v smernici Európskeho parlamentu a Rady (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/475/SVV a ktorou sa mení rozhodnutie Rady 2005/671/SVV (Ú. v. EÚ L 88, 31.3.2017, s. 6–21).
(7) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/784 z 29. apríla 2021 o riešení šírenia teroristického obsahu online (Text s významom pre EHP) (Ú. v. EÚ L 172, 17.5.2021, s. 79–109).
(8) Bližšie špecifikované v smernici Rady 2002/90/ES z 28. novembra 2002.

5. PRAKTICKÉ PRÍKLADY INDIKÁTOROV

Výbor sa domnieva, že indikátory podozrení z trestných činov, ktorých dôsledkom je ohrozenie života alebo bezpečnosti, môžu vyplývať buď priamo zo samotného obsahu alebo z obsahu v kombinácii s dodatočnými informáciami, ktoré má poskytovateľ k dispozícii. Príkladmi sú kontextové a technické informácie, prítomnosť identifikovateľnej obete (obetí) alebo miesta (miest) alebo oblasť odbornosti osoby alebo subjektu, ktorý poskytovateľa na tento obsah upozornil (napr. dôveryhodný nahlasovateľ špecializovaný na odhaľovanie konkrétnych typov nezákonného obsahu).

Na základe získanej spätnej väzby táto časť poskytuje (**nie úplný**) prehľad praktických príkladov obsahujúcich rôzne typy informácií, ktoré po manuálnom posúdení odborným a znalým hodnotiteľom vyvolávajú podozrenie z trestného činu, ktorého dôsledkom je ohrozenie života alebo bezpečnosti. Príklady sa týkajú rôznych typov hostingových služieb typu online platformy (napr. sociálne siete, herné platformy, diskusné fóra) a iných hostingových služieb (napr. chatové skupiny, služby zdieľania súborov, cloudové služby). Tieto praktické príklady sú fiktívne, avšak vychádzajú z reálnych zdokumentovaných prípadov.

Príklad 1 (Kategória: Trestné činy terorizmu, trestné činy proti ľudskosti a/alebo verejnej bezpečnosti)

Typ obsahu: Textový obsah (príspevky na sociálnej sieti).

Obsah: Podnecovanie k páchaniu násilných útokov, vrátane podpaľačských útokov na domy (*„do **** s deportáciami, poďme rovno na nich“*). Niektoré príspevky zdieľajú „zoznam cieľov“ s názvami konkrétnych miest a ich adresami.

Dodatočné informácie: Manuálne posúdenie príslušných používateľských účtov a interakcie používateľov s obsahom (vrátane podozrivých lokalít) potvrdzuje existenciu hodnovernej hrozby.

Príklad 2 (Kategória: Trestné činy proti životu a/alebo telesnej integrite osoby)

Typ obsahu: Textový a obrazový obsah (príspevky v uzavretej skupine na sociálnej sieti)

Obsah: Explicitné hrozby ublíženia na zdraví, vrátane vyobrazení noža, smerované voči konkrétnej osobe.

Dodatočné informácie: Manuálne posúdenie príslušného používateľského účtu, skupiny a interakcie s obsahom (vrátane komentárov) potvrdzuje existenciu hodnovernej hrozby.

Príklad 3 (Kategória: Trestné činy proti životu a/alebo telesnej integrite osoby)

Typ obsahu: Textový obsah (príspevky v diskusnom fóre)

Obsah: Opisy prebiehajúcich príprav na spáchanie streľby v škole.

Ďalšie informácie: Manuálne posúdenie príslušného používateľského účtu naznačuje, že účet sa nachádza v blízkosti školy. Opakované príspevky z tej istej IP adresy naznačujú vývoj a eskaláciu situácie v reálnom čase.

Príklad 4 (Kategória: Trestné činy proti sexuálnej integrite a/alebo sebaurčeniu osoby)

Typ obsahu: Textový obsah (správy v skupinovom chate, uložené v cloudovom hostingu)

Obsah: Podrobné informácie a pokyny k zakúpeniu fľaše s tekutinou „bez chuti a bez zápachu“ na omámenie osoby, pričom sa uvádza: *„Tvoja baba nič neucíti a nič si nebude pamätať.“*

Ďalšie informácie: Manuálne posúdenie skupinového chatu odhalilo, že obsahuje niekoľko správ z rôznych používateľských účtov, v ktorých sa zdieľajú praktické rady a pokyny, ako omámiť svojich partnerov s cieľom ich sexuálneho napadnutia a znásilnenia.

Príklad 5 (Kategória: Trestné činy proti sexuálnej integrite a/alebo sebaurčeniu osoby)

Typ obsahu: Textový obsah (príspevky v diskusnom fóre)

Obsah: Explicitné rady, ako nalákať maloleté osoby na výrobu sexuálne explicitného materiálu, ktorý sa následne použije na nátlak a vydieranie.

Ďalšie informácie: Na tento obsah upozornil dôveryhodný nahlasovateľ s odbornými znalosťami v oblasti boja proti online groomingu.

Príklad 6 (Kategória: Trestné činy proti slobode a ľudskej dôstojnosti)

Typ obsahu: Textový obsah (príspevky na sociálnej sieti)

Obsah: Násilné urážky namierené voči identifikovateľnej osobe, zverejnenie osobných údajov tejto osoby vo forme fotografie a adresy jej údajného bydliska a oznámenie, že používateľ na ňu bude čakať a *„postará sa o to, aby už nikdy nechodila“.*

Dodatočné informácie: Hoci sú informácie na prvý pohľad nejednoznačné, manuálne posúdenie príslušného používateľského účtu a jeho histórie potvrdzuje skutočnú udalosť a hodnovernú hrozbu.

Príklad 7 (Kategória: Trestné činy proti slobode a ľudskej dôstojnosti a trestné činy proti sexuálnej integrite osoby)

Typ obsahu: Obrazový obsah (video v uzavretej skupine na sociálnej sieti)

Obsah: Nadpis videa *„Došli nové kočky“,* vrátane záberov na prepravu a ukrývanie potenciálnych obetí obchodovania s ľuďmi na účely sexuálneho vykorisťovania.

Dodatočné informácie: Tento obsah nahlásila poskytovateľovi mimovládna organizácia, ktorá sa špecializuje na vyhľadávanie online obsahu naznačujúceho obchodovanie s ľuďmi. Manuálne posúdenie obsahu vrátane vizuálnej analýzy, metadát a histórie používateľského účtu potvrdzuje hodnovernú hrozbu.

Príklad 8 (Kategória: Trestné činy proti životu a/alebo telesnej integrite osoby)

Typ obsahu: Obrazový obsah (video vysielané naživo na hernej platforme)

Obsah: Živé vysielanie, v ktorom viacerí používatelia nabádajú a nútia iného používateľa k sebapoškodzovaniu. V živom vysielaní je vidieť nôž a lano.

Ďalšie informácie: Niekoľko používateľských účtov komentuje živé vysielanie a inštruuje vyobrazenú osobu, aby ublížila sebe, svojmu domácemu zvieraťu a členom rodiny.

Príklad 9 (Kategória: Trestné činy terorizmu, trestné činy proti ľudskosti a/alebo verejnej bezpečnosti)

Typ obsahu: Obrazový obsah (obrázky vo verejnom skupinovom chate prevádzkovanom poskytovateľom služby zasielania správ)

Obsah: Niekoľko obrázkov zobrazujúcich synagógu, strelné zbrane a strelivo, ako aj symboly extrémistickej ideológie.

Ďalšie informácie: Manuálne posúdenie obsahu, príslušného používateľského účtu a histórie jeho konverzácií poukazuje na používanie známych antisemitských kódových výrazov a skrytých narážok. Kontrola potvrdzuje skutočnú existenciu synagógy a reálnu hrozbu násilného útoku na toto miesto.

Príklad 10 (Kategória: Trestné činy proti sexuálnej integrite a/alebo sebaurčeniu osoby)

Typ obsahu: Obrazový obsah (obrázky v uzavretej skupine na sociálnej sieti)

Obsah: Intímne snímky osoby s opismi naznačujúcimi, že boli zhotovené a zdieľané bez súhlasu zobrazeného človeka (*„pozri ako ju ***** v spánku“* a *„...keď je vypnutá“*), ako aj s opismi naznačujúcimi prebiehajúce sexuálne zneužívanie („Napíš mi do komentára, čo mám s ňou robiť“).

Dodatočné informácie: Tento obsah nahlásil poskytovateľovi dôveryhodný oznamovateľ s odbornými znalosťami v oblasti online obsahu zobrazujúceho sexuálne zneužívanie.

Príklad 11 (Kategória: Trestné činy proti životu a/alebo telesnej integrite osoby)

Typ obsahu: Obrazový a textový obsah (priečinok s dokumentmi na webovej stránke na zdieľanie súborov)

Obsah: Príručky s návodmi a bezprostredne použiteľnými pokynmi na podpaľačstvo, bitie, bodanie (vrátane výberu bodných zbraní a častí tela, ktoré treba zasiahnuť), streľbu, výrobu improvizovaných výbušných zariadení a biologických zbraní (jedov a kontaminantov), spolu s operačnými a taktickými pokynmi.

Ďalšie informácie: Tento obsah nahlásil poskytovateľovi iný používateľský účet, ktorý získal odkaz na priečinok na inej službe (hernej platforme).

Príklad 12 (Kategória: Trestné činy terorizmu, trestné činy proti ľudskosti a/alebo verejnej bezpečnosti)

Typ obsahu: Obrazový obsah (obrázky vo verejnej skupine na sociálnej sieti)

Obsah: Videá a obrázky pravdepodobne zobrazujú a propagujú loď s výkonným motorom s cieľom odviezť osoby a umožniť im vstúpiť na územie členského štátu EÚ. Neuvádzajú sa žiadne informácie o imigračných alebo vízových požiadavkách a náklady na prepravu sú neprimerane vysoké. Zdá sa, že na lodi chýba záchranné vybavenie, ako sú záchranné vesty.

Dodatočné informácie: Manuálne posúdenie obsahu vrátane vizuálnej analýzy, metadát a súvisiaceho používateľského účtu potvrdzuje podozrenie z napomáhania neoprávnenému vstupu do členských štátov EÚ, čo predstavuje hodnoverné ohrozenie života a bezpečnosti osôb využívajúcich takúto prepravu. Z posúdenia vyplýva, že skupina obsahuje niekoľko príspevkov z rôznych používateľských účtov propagujúcich vstup na územie EÚ, a to vrátane cien, miest odchodu a kontaktných čísel.

Príklad 13 (Kategória: Trestné činy terorizmu, trestné činy proti ľudskosti a/alebo verejnej bezpečnosti)

Typ obsahu: Obrazový obsah (živé vysielanie na sociálnej sieti)

Obsah: Živé vysielanie, ktoré zrejme zachytáva osobu úmyselne jazdiacu vysokou rýchlosťou v protismere na diaľnici.

Dodatočné informácie: Manuálne posúdenie spôsobu jazdy, jej zjavného zámeru, rýchlosti a smeru potvrdzuje ohrozenie života alebo bezpečnosti účastníkov cestnej premávky a verejnosti vo všeobecnosti.

Príklad 14 (Kategória: Trestné činy proti životu a/alebo telesnej integrite osoby)

Typ obsahu: Zvukový obsah (hlasové správy v online hre pre viacerých hráčov)

Obsah: Konkrétne vyhrážky použitím strelnej zbrane a chválenie sa prístupom k strelným zbraniam a strelivu. Spomína sa miestne obchodné centrum.

Dodatočné informácie: Tento obsah nahlásil poskytovateľovi iný používateľský účet, pričom identifikoval autora správ a varoval pred plánovaným násilným útokom v obchodnom centre.

6. URČENIE DOKTNUTÉHO ČLENSKÉHO ŠTÁTU

Podľa článku 18 ods. 1 DSA sú poskytovatelia digitálnych služieb povinní informovať orgány presadzovania práva dotknutého členského štátu (dotknutých členských štátov). Článok 18 ods. 2 DSA stanovuje, že dotknutým členským štátom je ten členský štát, v ktorom má podozrivý páchateľ a/alebo obeť bydlisko alebo sa nachádza, ako aj miesto, kde sa podozrenie z trestného činu vyskytlo, vyskytuje alebo sa pravdepodobne vyskytne, vrátane prípadov, keď sa trestný čin spácha pri vstupe do členského štátu.

Na úvod je potrebné poznamenať, že v závislosti od typu poskytovaných hostingových služieb môžu mať poskytovatelia k dispozícii rôzne kategórie údajov, a preto by sa mal nasledujúci postup posudzovania považovať za uplatniteľný v danom kontexte.

6.1 Postup interného posudzovania

Na základe získanej spätnej väzby táto časť uvádza osvedčené postupy pre posudzovanie dostupných informácií poskytovateľmi na účely identifikácie dotknutého členského štátu (dotknutých členských štátov).

Interné posudzovanie môže zahŕňať preskúmanie samotného obsahu s cieľom zistiť akékoľvek náznaky miesta, kde sa podozrivý trestný čin stal, deje sa alebo sa pravdepodobne stane, ako aj miesta pobytu alebo bydliska podozrivého páchateľa alebo miesta pobytu alebo bydliska potenciálnej obete. Obsah sa napríklad môže už priamo odvolávať na určité miesto alebo poskytovať nepriame informácie, ako sú jazyk a nárečia, kontext, miestne orientačné body, konkrétne udalosti, podrobnosti, ako sú nápisy/plagáty/výrobky/tričká/elektrické zásuvky, prípadne typické trendy v konkrétnych oblastiach.

Ďalej môže interné posudzovanie zahŕňať preskúmanie technických informácií, ak sú k dispozícii, ako napríklad:

- IP adresa použitá pri nahrávaní obsahu s presným časovým údajom;
- história IP adries v priebehu času;
- údaje o geolokácii, napríklad GPS údaje v súvisiacich metadátach;
- základné informácie o účastníkovi (BSI), ako sú údaje o registrácii účtu, doručovacie adresy, fakturačné adresy, bankové údaje, telefónne číslo s národnou predvoľbou, e-mailové adresy s doménou najvyššej úrovne (s kódom krajiny).

Okrem toho môže interné posúdenie zahŕňať preskúmanie kontextových informácií, ak sú k dispozícii, napríklad:

- jazyk alebo jazyky používané v súvisiacom obsahu (napr. komentáre, popisy);
- jazyk alebo jazyky používané v názvoch súvisiacich používateľských účtov;
- jazyk alebo jazyky používané v súvisiacich názvoch adresárov/súborov;
- implicitné informácie v iných súvisiacich používateľských účtoch a obsahu.

6.2 Oznámenia, ktoré sa týkajú viacerých členských štátov

Dostupné informácie môžu naznačovať, že sa predmetné informácie týkajú viacerých členských štátov. Takéto informácie môžu napríklad uvádzať rôzne miesta pobytu potenciálnej obete a podozrivého páchateľa. Na základe získaných spätných informácií sa v takýchto prípadoch považuje za osvedčenú prax, aby boli upovedomené príslušné orgány presadzovania práva všetkých identifikovaných dotknutých členských štátov a aby oznámenie obsahovalo jasné informácie o tom, ktorý ďalší príslušný orgán bol súčasne informovaný.

6.3 Oznámenia, pri ktorých nie je možné s primeranou istotou identifikovať dotknutý členský štát

V súlade s článkom 18 ods. 2 DSA poskytovatelia hostingových služieb upovedomia orgány presadzovania práva v členskom štáte, v ktorom majú sídlo a/alebo Europol iba v prípade, ak dostupné informácie neposkytujú dostatočne presné určenie dotknutého členského štátu.

Preto ak poskytovateľ online služieb na základe dostupných informácií a interného posúdenia nie je schopný spoľahlivo identifikovať jeden alebo viac dotknutých členských štátov (napr. v dôsledku používania technológií na maskovanie polohy) alebo ak informácie naznačujú, že trestný čin sa týka výlučne tretej krajiny, poskytovatelia online služieb môžu ako záložné možnosti využiť členský štát, v ktorom sú usadení a/alebo Europol. Ako bolo uvedené vyššie, ak poskytovatelia hostingových služieb informujú obidva subjekty, oznámenie by malo obsahovať jasnú informáciu o tom, ktorý ďalší príslušný orgán bol súčasne informovaný.

7. POSKYTOVANIE RELEVANTNÝCH INFORMÁCIÍ

Podľa článku 18 ods. 1 DSA musia poskytovatelia hostingových služieb pri informovaní orgánov poskytnúť **všetky relevantné informácie**, ktorými disponujú. Vzhľadom na širokú škálu hostingových služieb, príslušného obsahu a dostupných informácií výbor konštatuje, že článok 18 DSA neposkytuje konečný či úplný zoznam takýchto informácií.

Recitál 56 DSA dodáva, že tieto informácie by mali **v prípade potreby** zahŕňať príslušný obsah a ak je to možné, aj čas zverejnenia obsahu vrátane určeného časového pásma, vysvetlenie podozrenia a informácie potrebné na lokalizáciu a identifikáciu príslušného príjemcu služby. Výbor tiež pripomína, že recitál 56 DSA stanovuje, že DSA neposkytuje právny základ na profilovanie príjemcov služieb na účely identifikácie trestných činov zo strany poskytovateľov. Poskytovatelia by zároveň pri informovaní orgánov mali dodržiavať aj ďalšie uplatniteľné pravidlá práva Únie alebo vnútroštátneho práva na ochranu práv a slobôd fyzických osôb.

Pri určovaní, ktoré relevantné informácie sa majú zdieľať, výbor preto považuje za osvedčenú prax, aby poskytovateľ zohľadnil najmä typ obsahu a trestného činu, ako aj mieru naliehavosti a dotknuté práva a slobody príslušných fyzických osôb, ako sú práva obetí[9], ako aj právo na ochranu údajov.

V praxi je hlavným účelom poskytovania dostupných informácií umožniť orgánom prijímajúcim oznámenia vykonať **potrebné** opatrenia, medzi ktoré patria najmä:

- priama reakcia na bezprostredné alebo pretrvávajúce ohrozenie života alebo bezpečnosti osoby alebo osôb;
- posúdenie trestnoprávnej relevantnosti oznámeného obsahu;
- prijatie vyšetrovacích opatrení, ako je vydanie alebo získanie príkazu na poskytnutie ďalších informácií na zaistenie dôkazov.

Výbor sa domnieva, že nasledujúce informácie sú pre orgány **potrebné a relevantné** na prijímanie opatrení. Ak je to možné, poskytovatelia by ich mali v rámci osvedčenej praxe poskytovať pri oznamovaní orgánom podľa článku 18 DSA:

- príslušný obsah (textový, obrazový alebo zvukový obsah v príslušných súborových formátoch, snímky obrazovky) a zodpovedajúce informácie na lokalizáciu obsahu v službe (napr. presná URL adresa alebo iné dostupné formáty, ak bol obsah odstránený alebo je nedostupný);
- údaj o tom, či je podľa interného posúdenia poskytovateľa ohrozenie života alebo bezpečnosti bezprostredné, či toto ohrozenie pretrváva alebo vyžaduje rýchlu reakciu orgánov vrátane údajov o prítomnosti identifikovateľnej obete (obetí) alebo miesta (miest);
- zhrnutie interného posúdenia poskytovateľa spolu s relevantnými informáciami, ako sú napríklad:
  - informácie na konkretizáciu príslušnej časti obsahu (napr. časová pečiatka videa), ak je to relevantné;
  - informácie o tom, či obsah nahlásil iný subjekt orgánom, ak je to relevantné;
  - informácie o tom, či príslušný používateľský účet vykazuje známky automatizovaného alebo koordinovaného neautentického správania, ak je to relevantné.

(9) Rada pripomína uplatňovanie smernice 2012/29, ktorou sa stanovujú minimálne normy v oblasti práv, podpory a ochrany obetí trestných činov a ktorá bola revidovaná smernicou 2026/1472, pokiaľ ide o akékoľvek informácie týkajúce sa obetí trestných činov, vrátane spracúvania ich osobných údajov.

V závislosti od informácií spracúvaných poskytovateľom, trestného činu a stupňa naliehavosti výbor zastáva názor, že oznámenie poskytovateľa by malo okrem vyššie uvedených informácií obsahovať podľa potreby a relevantnosti aj nasledujúce údaje:

- informácie na identifikáciu podozrivého páchateľa či páchateľov a/alebo potenciálnej obete či obetí, ako sú základné informácie o účastníkovi (napr. meno, e-mailová adresa, používateľské ID, telefónne číslo), zdrojová IP adresa použitá na prihlásenie a/alebo nahratie, technické informácie (napr. čas posledného prihlásenia, informácie o zariadení). Môžu sem patriť aj dostupné informácie o tretích stranách priamo spojených s podozrivým páchateľom (páchateľmi) a/alebo obeťou (obeťami), ak identifikácia nie je možná inými prostriedkami (napr. súvisiace alebo zdieľané používateľské účty, držitelia platobných prostriedkov používaných podozrivým páchateľom, držitelia telefónnych čísel používaných podozrivým páchateľom);
- informácie na lokalizáciu hrozby, ako napríklad zdrojová IP adresa použitá pri prihlasovaní užívateľa a/alebo nahratí obsahu, geolokačné údaje, fakturačná adresa, obsahové informácie, jazykové nastavenia;
- presné časové údaje o tom, kedy bol obsah nahraný a/alebo zverejnený vrátane časového pásma v UTC formáte (koordinovaný svetový čas);
- história používateľského účtu, napríklad odstránenie obsahu, pozastavenie účtu, opakované neprimerané správanie alebo existencia prepojených účtov.

Osvedčená prax: Uchovávanie relevantných informácií

WXZ Marketplace zistí, že určitý obsah naznačuje trestný čin, ktorého dôsledkom je ohrozenie bezpečnosti osoby. *WXZ Marketplace* okamžite zablokuje prístup k tomuto obsahu a bezodkladne informuje príslušný orgán v dotknutom členskom štáte. Hodnotiteľ manuálne preskúma dostupné údaje, vyberie a pripraví relevantné informácie a uchová ich na účely ich odoslania v reakcii na prípadné následné žiadosti alebo príkazy orgánov presadzovania práva alebo justičných orgánov, ak je to relevantné.

Na základe získanej spätnej väzby výbor považuje za osvedčenú prax, aby poskytovatelia zasielali relevantné informácie štruktúrovaným, štandardizovaným a konzistentným spôsobom. Pri poskytovaní informácií prostredníctvom webových portálov alebo rozhraní API je jasne štruktúrovaný formát poskytovaných údajov zvyčajne podmienený samotným použitým technickým rozhraním. Pokiaľ ide o poskytovanie informácií prostredníctvom iných zavedených kanálov, najmä e-mailom, výbor konštatuje, že poskytovatelia sa môžu spoliehať na dobrovoľné šablóny, napríklad zo strany vnútroštátnych orgánov.

Osvedčená prax: Poskytovanie relevantných informácií

Komunita WXZ zistí podozrenie na trestný čin, ktorého dôsledkom je ohrozenie života. Hodnotiteľ v bezpečnostnom tíme *komunity WXZ* manuálne preskúma dostupné informácie a posúdi, či predstavujú bezprostrednú alebo pretrvávajúcu hrozbu. Následne vyberie a odošle relevantné informácie orgánu identifikovaného členského štátu, pričom na oznámenie použije zavedený a konzistentný formát. *Komunita WXZ* zavádza automatizované systémy na zefektívnenie poskytovania informácií, avšak využíva manuálnu kontrolu a posudzovanie poskytovaných informácií.

8. OZNAMOVACIE A KOMUNIKAČNÉ KANÁLY

Zo získanej spätnej väzby vyplýva, že pri prijímaní oznámení sa orgány presadzovania práva, justičné orgány a Europol spoliehajú na e-mailovú komunikáciu a v niektorých prípadoch na webové portály zriadené na vnútroštátnej úrovni. Niektoré členské štáty navyše poskytujú vyhradené telefónne číslo na upozorňovanie orgánov o prichádzajúcom alebo odoslanom oznámení prostredníctvom zavedených kanálov s cieľom včas zmobilizovať potrebné zdroje. Takéto telefónne čísla by sa mali používať najmä na informovanie orgánov o bezprostredných alebo prebiehajúcich incidentoch v prípadoch, keď orgán nemonitoruje prijímanie oznámení nepretržite 24 hodín denne, 7 dní v týždni.

8.1 Jednotné kontaktné miesta (SPOC)

Výbor považuje za osvedčenú prax, aby orgány určili jednotné kontaktné miesta (SPOC), prípadne tieto už zriadené miesta udržiavali a zverejňovali, napríklad na webovej stránke. Jednotné kontaktné miesta môžu slúžiť ako prvý vstupný bod na posudzovanie a spracúvanie oznámení podľa článku 18 DSA a môžu disponovať kapacitami na nepretržité 24-hodinové monitorovanie, najmä s cieľom reagovať na bezprostredné alebo prebiehajúce hrozby.

Výbor berie na vedomie, že pracovná skupina č. 7 výboru vedie a pravidelne aktualizuje zoznam jednotných kontaktných miest. Komisia distribuuje tento zoznam poskytovateľom veľmi veľkých online platforiem (VLOPs). Výbor vyzýva koordinátorov, aby tento zoznam distribuovali poskytovateľom hostingových služieb usadených v ich členskom štáte. Komisia a koordinátori môžu, ak je to vhodné a s výslovným súhlasom zúčastnených strán, tieto informácie zverejniť na svojich príslušných webových stránkach, aby poskytovatelia mohli proaktívne identifikovať jednotné kontaktné miesta orgánov.

Okrem toho výbor považuje za osvedčenú prax, aby poskytovatelia hostingových služieb určili a verejne oznámili vlastné jednotné kontaktné miesto zodpovedné za komunikáciu a spoluprácu s orgánmi vo všetkých členských štátoch a s Europolom. V závislosti od veľkosti príslušného poskytovateľa a dostupných zdrojov môže takáto osoba alebo tím fungovať ako kontaktné miesto dostupné 24 hodín denne, 7 dní v týždni.

Zriadenie a operačná pripravenosť jednotných kontaktných miest zo strán orgánov aj poskytovateľov prispievajú k objasneniu úloh na oboch stranách, čo následne umožňuje rýchle a štruktúrované poskytovanie informácií a zároveň uľahčuje spätnú väzbu a žiadosti o informácie tam, kde je to potrebné.

Dobrovoľné partnerstvá

Získaná spätná väzba preukázala existenciu rôznych dobrovoľných partnerstiev, ako sú siete a neformálne fóra zahŕňajúce poskytovateľov aj orgány, ktorých cieľom je spoločne riešiť konkrétne typy nezákonného online obsahu alebo správania. Takéto partnerstvá môžu slúžiť aj ako podklad pre výmenu špecifických kontextových a jazykových informácií medzi poskytovateľmi a orgánmi vrátane oznamovacích kanálov zriadených na prijímanie oznámení podľa článku 18 DSA.

Osvedčená prax: Dobrovoľné partnerstvo medzi poskytovateľom a orgánmi

ABC Chat je online platforma prevádzkujúca diskusné miestnosti, zameriava sa na domáce publikum členského štátu, v ktorom je usadená, a ponúka službu výlučne v úradnom jazyku daného členského štátu. Služba je obzvlášť populárna medzi maloletými. Spoločnosť prevádzkujúca *ABC Chat* uzavrela dobrovoľné partnerstvo s príslušnými orgánmi v danom členskom štáte, ktoré sa zaoberá najmä riešením prípadov groomingu maloletých a sexuálneho vydierania v rámci tejto služby. Partnerstvo zahŕňa pravidelnú výmenu informácií o oznamovacích kanáloch, postupoch pri poskytovaní informácií, oblastiach trestnej činnosti špecifických pre danú službu a o nových hrozbách.

8.2 Technické riešenia pre poskytovanie informácií

Technické riešenia, ako sú webové portály alebo rozhrania API, sa považujú za užitočné, nakoľko umožňujú efektívne a štandardizované prijímanie oznámení. Výbor preto nabáda koordinátorov, aby zapojili poskytovateľov usadených v ich členskom štáte do využívania týchto riešení, ak je to možné.

Výbor tiež berie na vedomie, že Komisia spolupracuje s Europolom na podpore vývoja, údržby a prevádzky platformy, ktorá môže slúžiť ako celoeurópsky vstupný bod na prijímanie oznámení podľa článku 18 DSA.(10) Takáto platforma umožní štandardizované prijímanie oznámení vo všetkých členských štátoch. Výbor preto vyzýva koordinátorov, aby podporili prácu Komisie a Europolu s cieľom uľahčiť budúce zapojenie poskytovateľov hostingových služieb usadených v ich členskom štáte do tejto platformy.

8.3 Interakcia s inými oznamovacími povinnosťami

Výbor konštatuje, že iné právne predpisy Únie stanovujú podobné oznamovacie povinnosti ako článok 18 DSA. Ide najmä o článok 14 ods. 5 nariadenia (EÚ) 2021/784 (Nariadenie o riešení šírenia teroristického obsahu online – Nariadenie TCO), týkajúci sa teroristického obsahu predstavujúceho bezprostredné ohrozenie života a článok 9 nariadenia (EÚ) 2019/1148, týkajúci sa podozrivých transakcií, zmiznutí a odcudzení prekurzorov výbušnín na online trhoviskách.

Komisia analyzovala vzťah týchto ustanovení s článkom 18 DSA, a to v správe prijatej podľa článku 91 ods. 1 druhého pododseku DSA.(11) Najmä v prípade, ak sa poskytovateľ hostingových služieb dozvie o teroristickom obsahu, ktorý naznačuje bezprostredné ohrozenie života, má prednosť nariadenie TCO ako špecifickejšia povinnosť oznamovania teroristického obsahu.

Na základe získanej spätnej väzby výbor konštatuje, že v rámci osvedčenej praxe by poskytovatelia mali v oznámeniach jasne uvádzať konkrétnu oznamovaciu povinnosť (napr. s odkazom na článok 18 DSA). Poskytovatelia by zároveň s cieľom predísť duplicitným alebo protichodným reakciám zo strany orgánov nemali súbežne zasielať takéto oznámenia na základe samostatných oznamovacích povinností. Ak poskytovateľ napríklad zašle oznámenie podľa článku 14 ods. 5 nariadenia TCO, nie je potrebné dodatočne oznamovať rovnaký obsah podľa článku 18 DSA.

Okrem toho výbor zastáva názor, že keď poskytovateľ podľa článku 18 DSA oznámi orgánu podozrenie na teroristický alebo násilný extrémistický incident, môže to dotknutý orgán považovať za oznámenie o potenciálnej kríze na základe dobrovoľného mechanizmu „EU Online Crisis Response Framework“, ktorý slúži na prevenciu alebo obmedzenie šírenia nezákonného online obsahu súvisiaceho s podozrením na násilný extrémistický alebo teroristický útok. Tu je však potrebné dodať, že oznámenie podľa článku 18 DSA neznamená automatické spustenie tohto mechanizmu.

(10) Úprava platformy „PERCI“ (Plateforme Européenne de Retraits de Contenus Illégaux sur Internet)

(11) Správa Komisie pre Európsky parlament, Radu a Európsky hospodársky a sociálny výbor o uplatňovaní článku 33 nariadenia (EÚ) 2022/2065 a o interakcii tohto nariadenia s inými právnymi aktmi, SWD(2025) 268 final.

9. DOHĽAD NAD DODRŽIAVANÍM PREDPISOV

DSA nestanovuje žiadne povinnosti poskytovateľov hostingových podávať správy o transparentnosti zahŕňajúce oznámenia podľa článku 18. Výbor sa však domnieva, že transparentnosť pri prijímaní oznámení je kľúčovým predpokladom informovaného dohľadu nad dodržiavaním článku 18 DSA zo strany poskytovateľov.

Výbor odporúča, aby koordinátori viedli pravidelné konzultácie s orgánmi, ktoré prijímajú a spracúvajú oznámenia podľa článku 18 DSA. Orgány môžu napríklad vypracúvať správy v súlade s platnými obmedzeniami podľa vnútroštátneho trestného poriadku, ktoré obsahujú štatistiky o celkovom počte prijatých oznámení. Takéto správy môžu byť rozdelené napríklad podľa nasledujúcich kategórií:

- názov a typ poskytovateľa hostingovej služby (napr. sociálna sieť, platforma na zdieľanie videí, herná platforma);
- trestnoprávna relevantnosť z hľadiska ohrozenia života alebo bezpečnosti (napr. relevantné/nerelevantné);
- kvalita (dostatočné/nedostatočné informácie na to, aby orgán mohol podniknúť ďalšie kroky);
- geografická relevantnosť z hľadiska identifikácie dotknutého členského štátu (relevantné/nerelevantné);
- druh trestného činu (oblasť trestnej činnosti).

Okrem toho výbor konštatuje, že pripravovaná platforma na komunikáciu medzi Europolom, orgánmi presadzovania práva a poskytovateľmi hostingových služieb (pozri časť 8.2. vyššie) umožní získavať celoeurópske štatistické správy o oznámeniach zaregistrovaných na tejto platforme.

Osobitný význam pre dohľad nad dodržiavaním predpisov môžu predstavovať správy o transparentnosti podľa článku 15 DSA. Výbor preto vyzýva koordinátorov, aby zvážili analýzu týchto správ, konkrétne pokiaľ ide o oznámenia prijaté v súlade s článkom 16 DSA o mechanizmoch oznamovania a prijímania opatrení, ktoré sa môžu týkať príslušných trestných činov. Takéto správy o transparentnosti môžu prispieť k lepšiemu poznaniu rozsahu a pôsobnosti potenciálne relevantného nezákonného obsahu v súvislosti s článkom 18 DSA.

10. PREHĽAD DOKUMENTU

Tento dokument predstavuje osvedčené postupy a praktické príklady vychádzajúce zo spätnej väzby získanej pri doterajšom uplatňovaní článku 18 DSA. Dokument môže preto podliehať revíziám a aktualizáciám s ohľadom na praktické skúsenosti, nové trestné javy a vznikajúce trendy, nový technologický vývoj, nový vývoj v oblasti regulácie[12] a zmeny v prevádzkových štandardoch.

Výbor bude priebežne monitorovať účinnosť a relevantnosť tohto dokumentu a v prípade potreby ho spolupráci s Komisiou prehodnotí. Toto monitorovanie sa bude opierať aj o vytvorenie rámcov dohľadu, ktoré uľahčia pravidelné podávanie správ a transparentnosť týkajúcu sa prijímania oznámení podľa článku 18 DSA.

(12) Napríklad navrhované nariadenie, ktorým sa stanovujú pravidlá na prevenciu a boj proti sexuálnemu zneužívaniu detí, môže po prijatí a nadobudnutí účinnosti zaviesť povinnosť pre poskytovateľov hostingových služieb, aby v prípade, ak sa dozvedia o akýchkoľvek informáciách naznačujúcich potenciálne online šírenie materiálu zobrazujúceho sexuálne zneužívanie detí a navádzanie detí na sexuálne účely, bezodkladne podali hlásenie novozriadenému centru EÚ.