



EURÓPSKA
KOMISIA

V Bruseli 12. 9. 2018
SWD(2018) 409 final

PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE

ZHRNUTIE POSÚDENIA VPLYVU

Spríevodný dokument

Návrh nariadenia Európskeho parlamentu a Rady

o predchádzaní šíreniu teroristického obsahu online

{COM(2018) 640 final} - {SEC(2018) 397 final} - {SWD(2018) 408 final}

Súhrnný prehľad
Posúdenie vplyvu týkajúce sa predchádzania šíreniu teroristického obsahu online
A. Potreba konať
Prečo? Aký problém sa rieši?
Šírenie teroristického obsahu online zostáva aj naďalej významným a urgentným spoločenským a politickým problémom. Napriek početným neregulačným opatreniam sú hostingové služby online naďalej využívané na šírenie teroristického obsahu.
Čo sa od tejto iniciatívy očakáva?
Cieľom tejto iniciatívy je dosiahnuť väčšiu dôveru v prostredie online na jednotnom digitálnom trhu, a to tak, že sa obmedzí dostupnosť teroristického obsahu online a súčasne sa zabezpečí vysoká úroveň bezpečnosti občanov EÚ. Jej konkrétnym cieľom je zvýšiť účinnosť opatrení zameraných na odhaľovanie a odstraňovanie teroristického obsahu za súčasného zvýšenia transparentnosti a zodpovednosti poskytovateľov hostingových služieb. Iniciatíva sa zameriava aj na zlepšenie schopnosti príslušných orgánov zasiahnuť proti teroristickému obsahu online, na poskytnutie záruk proti riziku chybného odstránenia obsahu, ktorý nemá nezákonný charakter, ako aj na zabezpečenie náležitej ochrany základných práv.
Aká je pridaná hodnota opatrení na úrovni EÚ?
Väčšina online platforiem pôsobí cezhranične a umožňuje prístup k obsahu bez ohľadu na to, kde sa používatelia alebo poskytovatelia informácií nachádzajú. Členské štáty prijali právne predpisy v oblasti odstraňovania nezákonného obsahu online, avšak potreba zabezpečiť verejnú bezpečnosť na vnútroštátnej úrovni musí byť v rovnováhe so základnou slobodou poskytovať služby a slobodou usadiť sa v súlade s pravidlami jedného trhu. Začína vznikať nejednotný rámec vnútroštátnych pravidiel a hrozí, že táto nejednotnosť bude čoraz väčšia, čo by mohlo ohroziť účinné uplatňovanie slobody usadiť sa a slobody poskytovať služby v EÚ a súčasne aj obmedziť účinnosť boja proti teroristickému obsahu online, pretože nejednotné vnútroštátne pravidlá by viedli k zvýšeniu nákladov, ktoré by podniky museli vynakladať na ich dodržiavanie. Jednotlivé izolované opatrenia, ktoré prijímajú členské štáty, nemôžu účinným spôsobom riešiť otázku obmedzovania dostupnosti nezákonného obsahu online vzhľadom na povahu predmetných služieb a vzhľadom na začínajúcu fragmentáciu vnútorného trhu.
B. Riešenia
Aké legislatívne a nelegislatívne možnosti politiky sa zvažovali? Je niektorá z možností uprednostňovaná? Prečo?
V posúdení vplyvu sa okrem základného scenára zvažovali ďalšie tri možnosti, ktoré vychádzali z podobnej intervenčnej logiky, no líšili sa intenzitou, pokiaľ ide o účinnosť a vplyv na základné práva. Jednotlivé možnosti obsahujú tieto základné prvky: Ustanovenia na harmonizáciu postupov odstraňovania teroristického obsahu alebo znemožňovania prístupu k nemu na základe príkazu na odstránenie vydaného vnútroštátnym orgánom. Aby sa uvedené postupy mohli uplatňovať, harmonizovať sa musí aj spoločné vymedzenie pojmu teroristický obsah online (v každej z troch možností sa uvažuje o odlišnom vymedzení pojmu), ako aj ozrejmiť súdna náprava, ktorú môžu využiť poskytovatelia hostingových služieb a poskytovatelia obsahu v prípade, že chcú napadnúť príkaz na odstránenie (tento prvok je spoločný pre všetky tri možnosti). Ustanovenia na zabezpečenie transparentných postupov a transparentného podávania správ orgánom a Komisii (tieto ustanovenia sú podobné vo všetkých možnostiach) by viedli k zvýšeniu zodpovednosti a dôvery v postupy narábania s obsahom a podporili by tvorcov politik, ako aj vnútroštátne orgány v boji proti teroristickému obsahu. Popritom by umožnili používateľom lepšie pochopiť, ako poskytovatelia hostingových služieb uplatňujú svoje politiky riadenia obsahu.

Spolupráca medzi vnútroštátnymi orgánmi a s Europolom (v jednotlivých možnostiach sa miera tejto spolupráce líši) by prispela k zlepšeniu ich schopnosti podnikať kolektívne kroky proti teroristickému obsahu, pričom by sa predišlo duplicite a obmedzila by sa komplexnosť, ako aj náklady poskytovateľov hostingových služieb vyplývajúce z interakcie s vnútroštátnymi orgánmi, keď ponúkajú svoje služby cezhranične.

Okrem toho ustanovenia na zabezpečenie toho, aby poskytovatelia hostingových služieb v tých prípadoch, keď sú spoločnosti vystavené teroristickému obsahu, zaviedli **vhodné a primerané opatrenia na proaktívne odhaľovanie teroristického obsahu** (požiadavky v jednotlivých možnostiach sa líšia).

Záruky (spoločné pre všetky možnosti) a ustanovenia na zabezpečenie toho, aby opatrenia, ktoré sa prijali s cieľom odhaliť a odstrániť teroristický obsah, nevedli k chybnému odstráneniu obsahu, ktorý nie je nezákonný, a aby dodržiavali základné práva.

Ustanovenia **na zabezpečenie toho, aby boli opatrenia vykonateľné** (sú spoločné pre všetky možnosti), vrátane určenia právnych zástupcov v prípade spoločností mimo EÚ, vytvorenia kontaktných miest a zabezpečenia toho, aby mali členské štáty zavedený koherentný súbor sankcií.

V správe sa predkladá kombinácia opatrení, ktoré sa vyhodnotili ako najúčinnnejšie pri boji proti teroristickému obsahu online. V správe sa predkladá aj posúdenie výhod, ktoré ponúkajú rôzne základné prvky z hľadiska účinnosti.

V posúdení vplyvu sa dospelo k záveru, že začlenením nasledujúcich opatrení by sa dosiahla väčšia účinnosť pri dosahovaní politických cieľov: dôkladné vymedzenie pojmu teroristický obsah, zavedenie požiadaviek na odstránenie obsahu, ktorý je predmetom príkazu na odstránenie, do jednej hodiny, zavedenie požiadaviek na posúdenie hlásení od Europolu a členských štátov, ako aj požiadaviek na poskytovateľov hostingových služieb vystavených teroristickému obsahu, aby prijali proaktívne opatrenia na odhalenie nového teroristického obsahu a zabránili opätovnému nahrávaniu známeho materiálu, stanovenie solídneho súboru záruk proti chybnému odstráneniu obsahu, ktorý nie je nezákonný, a uloženie povinností súvisiacich s transparentnosťou.

Kto podporuje ktorú možnosť?

Poskytovatelia hostingových služieb vo všeobecnosti podporujú základný scenár a sú toho názoru, že najprv by sa mali plne zväžiť vplyvy neregulačného úsilia. Ak sa má prijať právny nástroj, v tom prípade podporujú intervenciu zameranú na konkrétne potreby s osobitným prínosom pre verejnosť.

Členské štáty uznávajú potrebu prijať ďalšie podporné opatrenia (t. j. neustály vývoj základného scenára) a podporujú intervenciu zameranú proti teroristickému obsahu. Členské štáty kládli dôraz najmä na potrebu zaviesť spoločné vymedzenie pojmu teroristický obsah, požiadavky, aby sa v nadväznosti na prijatie hlásenia konalo, proaktívne opatrenia, ako aj transparentnosť a opatrenia, ktoré uľahčia dostupnosť odstráneného obsahu na účely presadzovania práva. Európska rada vyzvala Komisiu, aby predložila legislatívny návrh na zlepšenie odhaľovania a odstraňovania obsahu, ktorý podnecuje k nenávisti a páchaniu teroristických činov.

Občianska spoločnosť zastupujúca digitálne práva, ako aj akademická obec podporili to, aby sa rozvíjal základný scenár. Odporúčali opatrnosť v súvislosti s niektorými prvkami zahrnutými do regulačných možností, najmä pokiaľ ide o proaktívne opatrenia a vplyvy na základné práva. Jednotlivci vyjadrili vo svojich odpovediach v rámci verejnej konzultácie rovnaké obavy. Reprezentatívna vzorka občanov odpovedajúcich na osobitný prieskum Eurobarometra podporila prijatie dodatočných opatrení na úrovni EÚ zameraných na nezákonný obsah online.

C. Náklady na uprednostňovanú možnosť a jej výhody

Toto posúdenie vplyvu obsahuje podrobný opis nákladov a výhod vyplývajúcich z opatrení navrhovaných v rámci každej možnosti. V posúdení vplyvu sa dospelo k názoru, že možnosť č. 3 je najúčinnnejšia. Tato možnosť by výrazne prispela k dosiahnutiu politických cieľov a priniesla by najväčšie výhody vzhľadom na rozsah a dosah problému. Hoci tretia možnosť by mala mať najväčší hospodársky vplyv z hľadiska očakávaných nákladov a dodatočnej administratívnej záťaže, zároveň by mala priniesť aj najväčšie výhody.

D. Nadväzná opatrenia

Kedy sa táto politika preskúma?

Na účely prípravy hodnotenia by sa mal vypracovať podrobný program monitorovania výstupov, výsledkov a vplyvov tohto nariadenia. Monitorovanie sa bude zakladať najmä na informáciách od členských štátov, ktoré budú zhromažďované príslušnými orgánmi počas výkonu ich povinností a ktoré budú doplnené o informácie z verejne dostupných správ vyhotovovaných na účely transparentnosti. Ostatné informácie, najmä o proaktívnych opatreniach, poskytnú poskytovatelia hostingových služieb v rámci svojich povinností podávať správy. Toto monitorovanie sa v prípade každej možnosti doplní o výskum, ktorý by mal prispieť k pochopeniu toho, ako sa šíri nezákonný obsah online, a ktorý by mal sledovať technologický vývoj automatizovaných nástrojov na odstraňovanie nezákonného obsahu.