EVROPSKÁ
KOMISE

V Bruselu dne 12.9.2018
SWD(2018) 409 final

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SOUHRN POSOUZENÍ DOPADŮ

Průvodní dokument k

návrhu nařízení Evropského parlamentu a Rady

o prevenci šíření teroristického obsahu online

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

Souhrnný přehled

Posouzení dopadů prevence šíření teroristického obsahu online

A. Potřeba opatření

Proč? Jaký problém se řeší?

Nárůst teroristického obsahu online i nadále představuje velký a palčivý společenský a politický problém. Vzdor řadě neregulativních opatření jsou k šíření takového obsahu stále využívány hostingové služby online.

Čeho by měla tato iniciativa dosáhnout?

Tato inciativa má za cíl posílit důvěru v internetové prostředí jednotného digitálního trhu tím, že omezí dostupnost teroristického obsahu online a současně zajistí občanům EU vysokou úroveň bezpečnosti. Konkrétně chce zvýšit účinnost opatření pro odhalování a odstraňování teroristického obsahu a také posílit transparentnost a odpovědnost poskytovatelů hostingových služeb. Opatření mají rovněž zlepšit schopnost příslušných orgánů zasahovat proti teroristickému obsahu online a poskytnout záruky proti riziku chybného odstranění zákonného obsahu i přiměřenou ochranu základních práv.

Jakou přidanou hodnotu budou mít tato opatření na úrovni EU?

Většina internetových platforem funguje napříč hranicemi a umožňuje přístup ke svému obsahu bez ohledu na to, kde se uživatelé nebo poskytovatelé informací nacházejí. Členské státy přijaly ve věci odstraňování nezákonného obsahu online právní předpisy, ale potřeba zajistit veřejnou bezpečnost na vnitrostátní úrovni musí být vyvážena základní svobodou poskytování služeb a svobodou usazování podle pravidel jednotného trhu.

Utváří se různorodá mozaika vnitrostátních pravidel či existuje riziko jejího rozrůstání. Takový vývoj by ohrozil účinné uplatňování svobody usazování a svobody poskytování služeb v EU a současně by snížil efektivitu boje proti teroristickému obsahu online, neboť touto různorodostí by se zvýšily náklady podniků na dodržování předpisů.

Prostřednictvím opatření pouze na úrovni jednotlivých členských států by se vzhledem k povaze dotčených služeb účinně nevyřešil úkol spočívající v omezení dostupnosti nezákonného obsahu online, ani problém vznikající roztříštěnosti vnitřního trhu.

B. Řešení

Jaké legislativní a nelegislativní možnosti byly zvažovány? Je některá možnost upřednostňována? Proč?

Posouzení dopadů zvažovalo kromě základního scénáře tři možnosti, které odrážejí podobnou logiku zásahu v různých stupních intenzity, pokud jde o efektivnost a dopad na základní práva. Základními prvky těchto možností mimo jiné jsou:

ustanovení k **harmonizaci postupů pro odstraňování teroristického obsahu nebo znemožnění přístupu k němu** na základě příkazu k odstranění od vnitrostátního orgánu. Aby se uvedené postupy mohly uplatňovat, musí se harmonizovat i **společná definice teroristického obsahu online** (v každé ze tří možností se uvažuje o odlišném vymezení pojmu) a vyjasnit otázka **soudní nápravy**, kterou mají poskytovatelé hostingových služeb a poskytovatelé obsahu k dispozici proti příkazům k odstranění (společné pro všechny tři možnosti).

Ustanovení k zajištění **transparentních postupů a transparentního podávání zpráv** orgánům a Komisi (podobné ve všech možnostech) by vedla k posílení odpovědnosti a důvěry v postupy usměrňování obsahu a podpořila by tvůrce politik a vnitrostátní orgány v boji proti teroristickému obsahu. Navíc by uživatelům pomohla lépe porozumět tomu, jak poskytovatelé hostingových služeb uplatňují svoje politiky řízení obsahu.

Spolupráce mezi vnitrostátními orgány a s Europolem (v jednotlivých možnostech se míra této spolupráce různí) by zlepšila jejich schopnost podnikat společné kroky proti teroristickému obsahu, přičemž by se zabránilo duplicitě a omezila se komplexnost, jakož i náklady poskytovatelů hostingových služeb vyplývající z interakce s vnitrostátními orgány při přeshraničním poskytování služeb.

Ustanovení mají navíc zajistit, že v případech, kdy jsou společnosti vystaveny teroristickému obsahu, zavedou poskytovatelé hostingových služeb **vhodná a přiměřená opatření k proaktivnímu odhalování teroristického obsahu** (požadavky s v jednotlivých možnostech různí).

Záruky (společné pro všechny možnosti) a ustanovení k zajištění, že opatření přijatá za účelem odhalení a odstranění teroristického obsahu nepovedou k chybnému odstranění zákonného obsahu a budou v souladu se základními právy.

Ustanovení **k zajištění, že budou opatření vymahatelná** (společné všem možnostem), včetně určení právních zástupců v případě společnosti mimo EU, zřízení kontaktních míst a zajištění, aby měly členské státy zavedený ucelený soubor sankcí.

Zpráva jako nejúčinnější prostředek pro boj proti teroristickému obsahu online prezentuje kombinaci posuzovaných opatření. Rovněž předkládá hodnocení výhod různých základních prvků z hlediska jejich účinnosti.

V posouzení dopadů se dospělo k závěru, že by se vyšší efektivity při plnění politických cílů dosáhlo začleněním takových opatření, jako je komplexní vymezení teroristického obsahu, zavedení požadavků na odstranění obsahu, který je předmětem příkazu k odstranění, do jedné hodiny, požadavků na posouzení hlášení Europolu a členských států, jakož i požadavků na poskytovatele hostingových služeb vystavených teroristickému obsahu, aby přijali proaktivní opatření k odhalení nového teroristického obsahu a zabránili opětovnému nahrávání známého materiálu, stanovení solidního souboru záruk proti chybnému odstranění obsahu, který není nezákonný, a uložení povinností souvisejících s transparentností.

Kdo podporuje kterou možnost?

Poskytovatelé hostingových služeb obecně podporují základní scénář a domnívají se, že nejdříve by se měly zvážit veškeré účinky neregulativních opatření. Má-li být přijat právní nástroj, podporují kroky zaměřené na konkrétní potřeby se zvláštním přínosem pro veřejnost.

Členské státy uznávají potřebu přijmout další podpůrná opatření (tj. pokračující rozvoj základního scénáře) a podporují kroky zaměřené proti teroristickému obsahu. Členské státy kladly důraz především na potřebu zavést společné vymezení pojmu teroristický obsah, požadavky na zákrok v případě nahlášení, proaktivní opatření, jako je transparentnost, a opatření, která usnadní dostupnost odstraněného obsahu pro účely prosazování práva. Evropská rada vyzvala Komisi, aby předložila legislativní návrh v zájmu zlepšení odhalování a odstraňování obsahu, jenž podněcuje k nenávisti a k páchání teroristických činů.

Občanská společnost zastupující digitální práva, jakož i akademická obec, podpořily rozvoj základního scénáře. Vyzvaly přitom k opatrnosti v souvislosti s některými prvky zahrnutými do regulativních možností, zejména pokud jde o proaktivní opatření a dopad na základní práva. Stejné obavy vyjádřili v rámci veřejné konzultace i jednotlivci. Reprezentativní vzorek občanů v odpovědi na zvláštní průzkum Eurobarometru podpořil přijetí dodatečných opatření na úrovni EU zaměřených proti nezákonnému obsahu online.

C. Náklady na upřednostňovanou možnost a její výhody

Toto posouzení dopadů obsahuje podrobný rozpis nákladů a výhod vyplývajících z opatření v rámci jednotlivých možností. Posouzení dospělo k závěru, že nejefektivnější je možnost 3. Výrazně by přispěla k dosažení politických cílů a přinesla by i největší výhody, pokud jde o rozsah a dosah celého problému. I když by třetí možnost dle předpokladů měla největší hospodářský dopad z hlediska očekávaných nákladů a dodatečné administrativní zátěže, zároveň by přinesla i největší výhody.

D. Návazná opatření

Kdy bude tato politika přezkoumána?

Pro účely přípravy hodnocení by měl být vypracován podrobný program monitorování výstupů, výsledků a dopadů daného právního předpisu. Monitorování bude vycházet zejména z informací od členských států, které budou shromažďovány příslušnými orgány během výhonu jejich povinností a které budou doplněny o informace z veřejně dostupných zpráv o transparentnosti. Ostatní informace, zejména o proaktivních opatřeních, poskytnou poskytovatelé hostingových služeb v rámci své povinnosti podávat zprávy. Toto monitorování se ve všech

možnostech doplní o výzkum, který má napomoci epšímu porozumění, jak se šíří nezákonný obsah online, a který by měl sledovat technologický vývoj automatizovaných nástrojů na odstraňování nezákonného obsahu.