KOMISJA
EUROPEJSKA

Bruksela, dnia 12.9.2018 r.
SWD(2018) 409 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE OCENY SKUTKÓW

Towarzyszący dokumentowi:

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady

w sprawie zapobiegania rozpowszechnianiu w internecie treści ocharakterze terrorystycznym

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

Streszczenie oceny skutków

Ocena skutków dotycząca zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym

A. Zasadność działań

Jak uzasadniono ten wybór lub jego brak? Na czym polega problem?

Rozprzestrzenianie treści o charakterze terrorystycznym w internecie jest nadal istotnym i pilnym problemem społecznym i politycznym. Pomimo szeregu środków nieregulacyjnych internetowe usługi hostingowe są nadal wykorzystywane do rozpowszechniania treści o charakterze terrorystycznym.

Jaki jest cel inicjatywy?

Celem tej inicjatywy jest zwiększenie zaufania do środowiska internetowego na jednolitym rynku cyfrowym przez ograniczenie dostępności treści o charakterze terrorystycznym w internecie, przy jednoczesnym zapewnieniu wysokiego poziomu bezpieczeństwa obywateli UE. W szczególności ma ona na celu zwiększenie skuteczności środków służących wykrywaniu i usuwaniu treści o charakterze terrorystycznym, przy jednoczesnym zwiększeniu przejrzystości i odpowiedzialności dostawców usług hostingowych. Środek ten zmierza również do poprawy zdolności właściwych organów do interwencji w odniesieniu do treści o charakterze terrorystycznym w internecie, do ochrony przed ryzykiem błędnego usunięcia legalnych treści, a także do odpowiedniej ochrony praw podstawowych.

Na czym polega wartość dodana podjęcia działań na poziomie UE?

Większość platform internetowych działa ponad granicami i umożliwia dostęp do treści niezależnie od lokalizacji użytkowników i dostawców informacji. Państwa członkowskie uchwaliły akty prawne w dziedzinie usuwania nielegalnych treści w internecie, ale należy zapewnić równowagę między koniecznością zapewnienia bezpieczeństwa publicznego na szczeblu krajowym a podstawową swobodą świadczenia usług i swobodą przedsiębiorczości w ramach przepisów dotyczących jednolitego rynku.

Pojawiają się lub mogą się rozrastać niejednolite ramy przepisów krajowych, co stanowiłoby zagrożenie dla skutecznego korzystania ze swobody przedsiębiorczości i swobody świadczenia usług w UE, a jednocześnie ograniczyłoby skuteczność zwalczania treści o charakterze terrorystycznym w internecie, ponieważ przepisy takie doprowadziłyby do wzrostu kosztów przestrzegania przepisów dla przedsiębiorstw.

Ze względu na charakter przedmiotowych usług i powstające rozdrobnienie rynku wewnętrznego działania podejmowane wyłącznie przez państwa członkowskie nie mogą skutecznie sprostać wyzwaniu, jakim jest ograniczenie dostępności nielegalnych treści w internecie.

B. Rozwiązania

Jakie warianty legislacyjne i nielegislacyjne rozważono? Czy wskazano preferowany wariant? Jak uzasadniono ten wybór lub jego brak?

W ocenie skutków rozważono trzy warianty oprócz scenariusza odniesienia, które odzwierciedlają podobną logikę interwencji o różnym stopniu intensywności pod względem skuteczności i wpływu na prawa podstawowe. Elementy składowe wariantów obejmują:

Przepisy mające na celu **harmonizację procedur usuwania lub uniemożliwiania dostępu do treści o charakterze terrorystycznym** po wydaniu przez organ krajowy nakazu usunięcia. Aby umożliwić stosowanie procedur, harmonizacja obejmuje również **wspólną definicję treści o charakterze terrorystycznym w internecie** (różne definicje rozważane w ramach tych trzech wariantów), a także przejrzystość w odniesieniu do **możliwości odwołania się do sądu** od nakazu usunięcia dostępnych dla dostawców usług hostingowych i dostawców treści (wspólnych dla wszystkich wariantów).

Przepisy mające na celu zapewnienie **przejrzystości procesów i sprawozdań** dla organów i Komisji (podobne we wszystkich wariantach) zwiększyłyby odpowiedzialność i zaufanie do procesu moderacji treści oraz wspierałyby decydentów i organy krajowe w zwalczaniu treści o charakterze terrorystycznym, a ponadto pomagałyby użytkownikom lepiej zrozumieć to, jak dostawcy usług hostingowych stosują swoją politykę

zarządzania treścią.

Współpraca organów krajowych i Europolu (o różnej intensywności, zależnie od wariantu) poprawiłaby ich zdolność do wspólnego działania wymierzonego w treści o charakterze terrorystycznym, pozwoliłaby uniknąć powielania działań, a ponadto dzięki niej dostawcy usług hostingowych oferujący usługi transgraniczne, którzy kontaktują się z organami krajowymi, ponosiliby mniejsze koszty i stosowaliby mniej skomplikowane procedury.

Ponadto przepisy gwarantujące, że w przypadkach, gdy przedsiębiorstwa są narażone na treści o charakterze terrorystycznym, dostawcy usług hostingowych wprowadzają **odpowiednie i proporcjonalne środki w celu proaktywnego wykrywania treści o charakterze terrorystycznym** (różne wymogi w różnych wariantach).

Gwarancje (wspólne dla wszystkich wariantów) oraz przepisy mające na celu zapewnienie, by środki wdrażane w celu wykrywania i usuwania treści o charakterze terrorystycznym nie prowadziły do błędnego usuwania treści legalnych i były zgodne z prawami podstawowymi.

Przepisy mające **zagwarantować, by środki były wykonalne** (wspólne dla wszystkich wariantów), w tym ustanowienie przedstawicieli prawnych dla przedsiębiorstw spoza UE, ustanowienie punktów kontaktowych i zapewnienie, by państwa członkowskie miały spójny zestaw sankcji.

W sprawozdaniu przedstawiono kombinację środków ocenionych jako najbardziej skuteczne w zwalczaniu treści o charakterze terrorystycznym w internecie. Przedstawiono w nim również ocenę korzyści pod względem skuteczności wynikających z różnych elementów składowych.

W ocenie skutków stwierdzono, że bardziej skuteczne w osiąganiu celów polityki byłoby włączenie środków takich jak kompleksowa definicja treści o charakterze terrorystycznym, wymogi dotyczące usuwania za pomocą nakazu usunięcia oznaczonych treści w ciągu jednej godziny i oceny zgłoszeń zarówno od Europolu, jak i od państw członkowskich, a także wymogi, by dostawcy usług hostingowych narażeni na treści o charakterze terrorystycznym wprowadzali proaktywne środki w celu wykrycia nowych treści o charakterze terrorystycznym i zapobiegania ponownemu zamieszczeniu znanego materiału, jak również solidny zestaw gwarancji zapobiegających błędnemu usuwaniu treści legalnych i obowiązki w zakresie przejrzystości.

Jak kształtuje się poparcie dla poszczególnych wariantów?

Dostawcy usług hostingowych ogólnie popierają scenariusz odniesienia; uważają oni, że należy w pierwszej kolejności ocenić pełne skutki działań nieregulacyjnych. Jeżeli instrument prawny zostanie przyjęty, opowiadają się za ukierunkowaną interwencją w określonych obszarach o szczególnej wartości publicznej.

Państwa członkowskie uznają potrzebę wprowadzenia dalszych środków wspierających (tj. dalszego rozwoju scenariusza odniesienia) i popierają interwencję wymierzoną w treści o charakterze terrorystycznym. Państwa członkowskie podkreśliły w szczególności, że konieczne są: wspólna definicja treści o charakterze terrorystycznym, wymogi dotyczące podejmowania działań po otrzymaniu zgłoszenia, proaktywne środki, a także przejrzystość i ułatwienie – do celów egzekwowania prawa – dostępu do treści usuniętych. Rada Europejska wezwała Komisję do przedstawienia wniosku ustawodawczego służącego poprawie wykrywania i usuwania treści podżegających do nienawiści i do działań terrorystycznych.

Społeczeństwo obywatelskie reprezentujące prawa cyfrowe i środowiska akademickie wyraziło poparcie dla zmian scenariusza odniesienia. Grupa ta opowiedziała się za zachowaniem ostrożności w odniesieniu do niektórych elementów składowych wariantów regulacyjnych, w szczególności w odniesieniu do proaktywnych środków i skutków dla praw podstawowych. W odpowiedziach przesłanych w ramach konsultacji społecznych osoby fizyczne podzieliły te obawy; reprezentatywna próba obywateli, którzy odpowiedzieli na specjalne badanie Eurobarometr, poparła dodatkowe środki na szczeblu UE w dziedzinie zwalczania nielegalnych treści w internecie.

C. Koszty i korzyści preferowanego wariantu

Niniejsza ocena skutków zawiera szczegółowe informacje na temat kosztów i korzyści związanych ze środkami ujętymi w każdym wariancie. Z oceny wynika, że wariant 3 jest najbardziej skuteczny. Ten wariant strategiczny przyczyniłby się w znacznym stopniu do osiągnięcia celów polityki i przyniósłby największe korzyści w stosunku do skali i zakresu problemu. Chociaż oczekuje się, że trzeci wariant będzie miał największy wpływ na gospodarkę w odniesieniu do spodziewanych kosztów i dodatkowych obciążeń administracyjnych, przyniósłby on również największe korzyści.

D. Działania następcze

Kiedy nastąpi przegląd przyjętej polityki?

Na potrzeby oceny zostanie opracowany szczegółowy program monitorowania produktów, rezultatów i skutków prawodawstwa. Monitorowanie będzie opierało się głównie na informacjach pochodzących od państw członkowskich, zebranych przez właściwe organy w trakcie wykonywania ich obowiązków, a uzupełnią je publicznie dostępne sprawozdania na temat przejrzystości. Inne dane, w szczególności te dotyczące proaktywnych środków, będą dostarczane przez dostawców usług hostingowych w ramach ich obowiązków sprawozdawczych. Monitorowanie to, we wszystkich wariantach, zostanie uzupełnione badaniami mającymi na celu lepsze zrozumienie rozpowszechniania w internecie nielegalnych treści, a także śledzeniem rozwoju technologicznego w zakresie zautomatyzowanych narzędzi do usuwania nielegalnych treści.