

**INSTRUKCJA DLA PRZEDSTAWICIELA POLSKI**  
**na spotkanie Radców JHA w dniu 22 listopada 2018 r. w Brukseli dotyczącego projektu**  
**rozporządzenia w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze**  
**terrorystycznym**

Uzgodniona z: MSWiA, MS, MON, MPiT, MF, MSZ, ABW, UKE, NASK, MC - DT, MC – DC

Jak wskazuje się w dokumencie 14519/18 głównym tematem spotkania ma być art. 15 i motyw 34 rozporządzenia. W miarę potrzeby dyskusji ma być poddany także art. 13 i motywy od 27 do 31, podobnie jak art. 18 i odpowiedni motyw 38.

Stanowisko Rządu RP do projektu rozporządzenia w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym nie zostało jeszcze skierowane do rozpatrzenia przez Komitet do Spraw Europejskich – zostanie przekazane wkrótce.

W trakcie dyskusji nad rozporządzeniem proponujemy wykorzystanie następującego stanowiska.

**Artykuł 15 i motyw 34 - jurysdykcja**

- **Należy zapewnić ochronę wolności wypowiedzi tj. zadbać by tworzone mechanizmy nie doprowadziły do zjawiska nadmiernego usuwania treści**, które nie mają charakteru propagandy terrorystycznej. Dlatego potrzebny jest mechanizm efektywnego nadzoru nad wydawaniem decyzji zobowiązujących dostawców usług hostingowych do usunięcia danej treści, tak by wykluczyć przypadki bezzasadnej cenzury.
- Prawo do środka odwoławczego może pozostać martwe, w przypadkach, w których strona zostanie zablokowana lub jej treść usunięta przez organ innego państwa niż to, w którym usługodawca prowadzi działalność. Dochodzenie swoich praw przed sądem innego państwa może bowiem wiązać się z poniesieniem nieproporcjonalnie wysokich kosztów.
- W związku z powyższym Holandia zaproponowała rozwiązanie, zgodnie z którym dostawcy będą mogli odwołać się od decyzji organu innego państwa przed sądem krajowym, w którym znajduje się główne miejsce prowadzenia przez niego działalności. Takie rozwiązanie jest jednak problematyczne w kontekście zakresu jurysdykcji sądów krajowych, ograniczonej zasadniczo do decyzji wydanych przez organy własnego państwa.
- W tym kontekście sugeruje się wprowadzenie w rozporządzeniu zmian zmierzających do zapewnienia, aby co do zasady właściwe organy danego państwa podejmowały decyzje o usunięciu treści lub zablokowaniu strony w odniesieniu do dostawców operujących na terytorium tego samego państwa. W związku z powyższym zasadne wydaje się doprecyzowanie określonych w art. 13 mechanizmów współpracy między organami właściwymi wyznaczonymi w poszczególnych państwach, tak aby możliwe było skuteczne

przekazywanie informacji o stronach, w odniesieniu do których konieczne jest podjęcie decyzji o ich zablokowaniu lub usunięciu treści.

#### **Dodatkowe uzasadnienie do stanowiska dotyczącego artykułu 15 i motywu 34**

Rozpatrując przepisy rozporządzenia należy zwrócić uwagę na koszty funkcjonowania projektowanego przez Komisję Europejską systemu usuwania i blokowania treści terrorystycznych w internecie. Koszty te mogą okazać się niebagatelne i tworzą ryzyko obniżenia konkurencyjności w szczególności małych dostawców. Wniosek będzie powodował konieczność poniesienia dodatkowych wydatków przez dostawców usług hostingowych, tak aby mogli oni spełnić wymogi stawiane im w rozporządzeniu. Dla działania systemu usługodawcy będą w praktyce musieli stworzyć punkt kontaktowy, dostępny w trybie 24/7, który zapewni ciągłą możliwość sprawnego kontaktu z właściwym organem państwowym. Dodatkowo pojawiają się także obowiązki sprawozdawcze, czy też konieczność przechowywania zablokowanych treści w celach dowodowych. Dodatkowe koszty będzie także generowało ewentualne zastosowanie mechanizmów filtrowania treści terrorystycznych. Rozporządzenie zakłada szacowanie ryzyka i pod tym kątem uwzględnianie sytuacji ekonomicznej poszczególnych hostingodawców. Dokładne koszty będą zależne od skali prowadzonej przez danego hostingodawcę działalności. Należy się jednak spodziewać wzrostu kosztów prowadzenia działalności przez tych usługodawców. Może to być stosunkowo większym obciążeniem dla mniejszych dostawców skutkując obniżeniem konkurencyjności cenowej świadczonych przez nich usług. Warto zwrócić uwagę, że z oceny skutków regulacji, którą przedstawiła Komisja Europejska do rozpatrywanego rozporządzenia wynika, że gros podmiotów, do których będą miały zastosowanie przepisy rozporządzenia to mali przedsiębiorcy. Z uwagi na szerokość przyjętej definicji, szacuje się, że obowiązkami wynikającymi z projektowanego aktu prawnego będzie objętych 10,5 tys. dostawców usług hostingowych mających siedzibę w Europie i prawie 20 000 mających siedzibę zarówno w Europie, jak i w USA i Kanadzie. Dlatego oceniając proponowaną legislację nie można ignorować skutków, jakie może wywołać to rozporządzenie na gospodarkę – w postaci obniżenia konkurencyjności małych dostawców. Duzi gracze poradzą sobie bowiem z dodatkowymi obciążeniami – dla małych rozporządzenie może się natomiast okazać dodatkową barierą w prowadzeniu działalności blokującą innowacyjność i dopływ nowych firm na rynek.

W rozporządzeniu – motyw 8 – wskazuje się, że: „Każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed właściwym sądem krajowym przeciwko wszelkim środkom wprowadzonym na podstawie niniejszego rozporządzenia, które mogą negatywnie wpłynąć na prawa tej osoby. Prawo to obejmuje w szczególności możliwość skutecznego zaskarżenia nakazów usunięcia przez dostawców usług hostingowych i dostawców treści przed sądem państwa członkowskiego, którego organy wydały nakaz usunięcia”. Prawo do środka odwoławczego – jeżeli będzie się wiązało z poniesieniem nieproporcjonalnie wysokich kosztów pozostanie martwe.

#### **Artykuł 13 i motywy 27 do 31 - współpraca między dostawcami usług hostingowych, właściwymi organami oraz, w stosownych przypadkach, odpowiednimi organami Unii**

- **Pozytywnie oceniamy rozwiązanie zaproponowane w art. 13 ust. 3**, które zakłada, że państwa członkowskie i dostawcy usług hostingowych mogą zdecydować się na wykorzystanie specjalnych narzędzi, w tym, w stosownych przypadkach, narzędzi ustanowionych przez odpowiednie organy Unii, takie jak Europol, w celu m.in. przetwarzania i informacji zwrotnych

dotyczących nakazów usunięcia na podstawie art. 4. **W tym kontekście istotne jest zapewnienie, aby zakres współpracy był w pełni zgodny z mandatem Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol).**

- **W odniesieniu do art. 13 i zakładanej w motywach 27 – 30 współpracy pomiędzy właściwymi organami państw członkowskich rodzą się wątpliwości. Co w przypadku gdy pojawią się problemy we współpracy?** Jak działać w przypadku, gdy organ jednego państwa członkowskiego ma odmienne stanowisko w danej sprawie niż jego odpowiednik w drugim państwie członkowskim – np. jeden domaga się usunięcia danych treści, a drugi uważa, że nie są to treści terrorystyczne i nie trzeba ich usuwać.

#### **Artykuł 18 i motyw 38 – Sankcje**

- **Dalszych wyjaśnień wymaga kwestia wyznaczenia właściwych organów odpowiedzialnych za egzekwowanie przepisów rozporządzenia**, o których mówi się art. 17 rozporządzenia – m.in. organu odpowiedzialnego za nakładanie sankcji przewidzianych w artykule 18.
- **Mając na uwadze, że to do państw członkowskich będzie należało wyznaczenie organów odpowiedzialnych za egzekwowanie rozporządzenia powstaje pytanie czy powinny to być organy śledcze, kontrwywiadowcze, czy też centralne organy administracji rządowej.** Odpowiednie organy powinny zostać zidentyfikowane odpowiednio wcześniej, chociażby z uwagi na konieczność zapewnienia gotowości organizacyjnej na realizację określonych w projekcie zadań.
- **Rozważenia wymaga, czy w ramach proponowanego wniosku nie należy zapewnić definicji organów właściwych pozostawiając państwu swobodę w zakresie ich wyznaczenia.**
- **Odnoszą się do sankcji należy mieć na względzie jednolitość przyjmowanych rozwiązań.** W motywie 38 wskazuje się, że to państwa członkowskie powinny przyjąć przepisy dotyczące sankcji, w tym, w stosownych przypadkach, wytyczne w sprawie nakładania kar pieniężnych. To będzie powodowało fragmentację rynku cyfrowego – poprzez przyjmowanie różnych wytycznych w poszczególnych państwach członkowskich.

#### **Informacje dodatkowe**

**Stanowisko rządu do projektu rozporządzenia w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym nie zostało jeszcze przyjęte. W Ministerstwie Cyfryzacji trwają prace nad jego przygotowaniem.** W tej sprawie współpracujemy z innymi resortami. Prowadziliśmy także konsultacje publiczne. **Stanowisko zostanie wkrótce przesłane do Komitetu Spraw Europejskich obsługiwane przez Ministerstwo Spraw Zagranicznych.**

**Głównym celem rozporządzenia jest stworzenie mechanizmu zapobiegania rozpowszechnianiu treści terrorystycznych w internecie poprzez ich jak najszybsze usuwanie i zapobieganie ponownemu umieszczeniu w sieci.**

**Rozporządzenie tworzy model współpracy pomiędzy właściwymi organami państwowymi zgłaszającymi treści terrorystyczne do usunięcia, a podmiotami świadczącymi usługi hostingu.** Zakres podmiotów objętych rozporządzeniem jest szeroki i obejmuje platformy społecznościowe, platformy umożliwiające umieszczanie treści wideo, audio i obrazów, wymianę plików, strony internetowe, na których użytkownicy mogą zamieszczać komentarze lub recenzje.

**W projekcie - art. 4., przewiduje się, że usługodawcy będą mieli obowiązek usuwania lub blokowania dostępu do treści terrorystycznych w ciągu 1 godziny od momentu otrzymania stosownego nakazu od uprawnionego organu państwa.** Ustawiczne niestosowanie się do nakazu usunięcia treści może wiązać się z sankcją finansową w wysokości nawet do 4 proc. rocznego obrotu dostawcy usług hostingowych.

Innym rozwiązaniem jest możliwość nałożenia na usługodawców obowiązku filtrowania i automatycznego blokowania treści terrorystycznych – art. 6. W art. 5 przewidziano natomiast możliwość skierowania, przez właściwy organ państwa lub Unii Europejskiej, zgłoszenia do dostawcy usług hostingowych. W oparciu o otrzymane zgłoszenie, to dostawca usługi będzie mógł podjąć decyzje, czy dany komunikat stanowi treść terrorystyczną i w związku z tym powinien zostać usunięty.

**Po stronie państw członkowskich będzie leżało wyznaczenie organu odpowiedzialnego za wydawanie nakazów usunięcia treści terrorystycznych oraz nadzór nad realizacją przestrzegania rozporządzenia przez usługodawców.**

**Wniosek legislacyjny będzie powodował konieczność poniesienia dodatkowych wydatków przez dostawców usług hostingowych, tak aby mogli oni spełnić wymogi stawiane im w rozporządzeniu.** Dla działania systemu usługodawcy będą w praktyce musieli stworzyć punkt kontaktowy, dostępny w trybie 24/7, który zapewni ciągłą możliwość sprawnego kontaktu z właściwym organem państwowym. Dodatkowo pojawiają się także obowiązki sprawozdawcze, czy też konieczność przechowywania zablokowanych treści w celach dowodowych. Dodatkowe koszty będzie także generowało ewentualne zastosowanie mechanizmów filtrowania treści terrorystycznych. **Może to być stosunkowo większym obciążeniem dla mniejszych dostawców skutkując obniżeniem konkurencyjności cenowej świadczonych przez nich usług.**

Warto zwrócić uwagę, że z oceny skutków regulacji, którą przedstawiła Komisja Europejska do rozpatrywanego rozporządzenia wynika, że **gros podmiotów, do których będą miały zastosowanie przepisy rozporządzenia to mali przedsiębiorcy. Z uwagi na szerokość przyjętej definicji, szacuje się, że obowiązkami wynikającymi z projektowanego aktu prawnego będzie objętych 10,5 tys. dostawców usług hostingowych mających siedzibę w Europie i prawie 20 000 mających siedzibę zarówno w Europie, jak i w USA i Kanadzie.** Dlatego oceniając proponowaną legislację nie można ignorować skutków, jakie może mieć to rozporządzenie na gospodarkę – w postaci obniżenia konkurencyjności małych dostawców. Duzi gracze poradzą sobie bowiem z dodatkowymi obciążeniami – dla małych rozporządzenie może się natomiast okazać dodatkową barierą w prowadzeniu działalności blokującą innowacyjność i doływ nowych firm na rynek.

Problematycznym może być także konflikt projektowanego rozporządzenia z przepisami Dyrektywy o handlu elektronicznym - w Polsce implementowanej w ramach ustawy o świadczeniu usług drogą elektroniczną. W szczególności istotne są dwa artykuły projektowanego aktu prawnego:

- Art. 6 projektowanego rozporządzenia zakłada możliwość nałożenia na dostawców usług hostingu ogólnego obowiązku monitorowania informacji pod kątem treści terrorystycznych. Oznacza to stosowanie mechanizmów filtrowania treści i de facto odstępstwo od art. 15 ust. 1 dyrektywy 2000/31/WE<sup>1</sup>. Artykuł 15 zakazuje państwom członkowskim nakładania na usługodawców ogólnego obowiązku monitorowania informacji.
- Art. 4 rozporządzenia zakłada usunięcie lub zablokowanie treści o charakterze terrorystycznym lub uniemożliwiają dostępu do nich w ciągu jednej godziny od momentu otrzymania nakazu usunięcia. Z kolei art. 14 dyrektywy o handlu elektronicznym wskazuje, że hostingodawca nie jest odpowiedzialny za informacje przechowywane na żądanie usługobiorcy, pod warunkiem że podejmuje niezwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do informacji, gdy uzyska takie wiadomości lub zostanie o nich powiadomiony.

---

<sup>1</sup> Artykuł 15 Brak ogólnego obowiązku w zakresie nadzoru

1. Państwa Członkowskie nie nakładają na usługodawców świadczących usługi określone w art. 12, 13 i 14 ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność.

2. Państwa Członkowskie mogą ustanowić w stosunku do usługodawców świadczących usługi społeczeństwa informacyjnego obowiązek niezwłocznego powiadamiania właściwych władz publicznych o rzekomych bezprawnych działaniach podjętych przez ich usługobiorców lub przez nich przekazanych informacjach lub obowiązek przekazywania właściwym władzom, na ich żądanie, informacji pozwalających na ustalenie tożsamości ich usługobiorców, z którymi mają umowy o przechowywanie.