Warszawa, 27 listopada 2018 r.

WKŁAD DO INSTRUKCJI DLA PRZEDSTAWICIELA POLSKI
na posiedzenie COREPER II w dniu 28 listopada 2018 r.

Przekazany do uzgodnień pomiędzy następującymi instytucjami: MSWiA, MS, MON, MPiT, MF, MSZ, ABW, UKE, NASK.

Justice and Home Affairs

b) Regulation on preventing the dissemination of terrorist content online
General approach
Instytucja wiodąca: MC
Rozpatrywany dokument: 14570/18

Stanowisko Polski do zaprezentowania podczas posiedzenia:
Przedstawiciel Polski sprzeciwi się przyjęciu podejścia ogólnego.

Stanowisko Polski do zaprezentowania w przypadku dyskusji:

- Polska **popiera działania służące ograniczaniu zasięgu oddziaływania propagandy terrorystycznej.** Tego rodzaju treści sprzyjają radykalizacji postaw i mogą inspirować do przygotowywania ataków. Z tego względu pożądane jest zajęcie się tym zagadnieniem w sposób kompleksowy, mając przy tym na względzie zapewnienie odpowiedniej równowagi pomiędzy potrzebami związanymi z zapewnieniem bezpieczeństwa a prawami podstawowymi. Popierając tak określony cel mamy jednak zastrzeżenia co do rozporządzenia w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym. Z tego względu **Polska sprzeciwia się przyjmowaniu podejścia ogólnego do projektowanego rozporządzenia.**
- **Wciąż prowadzimy analizę tekstu rozporządzenia – stanowisko Rządu RP jest na etapie uzgodnień pomiędzy resortami – dlatego zgłaszamy zastrzeżenia analityczne. Uważamy, że powinniśmy dostać więcej czasu na analizę tego aktu prawnego.**
- Nowa regulacja obejmuje swym zakresem platformy technologiczne niezależnie od skali ich działalności, czy poziomu rozwoju technologicznego. Dlatego uważamy, że **należy wziąć pod uwagę, czy rzeczywiście powinno się stosować takie samo podejście do globalnych koncernów, jak i małych firm działających lokalnie. Takie podejście nie jest brane wystarczająco pod uwagę w projekcie legislacyjnym.**
- W szczególności artykuł 4 rozporządzenia przewiduje, że hostingodawca będzie miał obowiązek usunięcia lub zablokowania treści w ciągu 1 godziny od otrzymania zgłoszenia. Co do zasady 1 godziny od momentu otrzymania nakazu ze strony właściwego organu jest zbyt restrykcyjny. 1 godzina, ze względów technicznych i organizacyjnych to zdecydowanie zbyt krótki okres na reakcję ze strony dostawcy. Oznacza to, że **usługodawca będzie musiał zapewnić punkt kontaktowy gotowy na reakcję i dostępny w trybie 24 godziny na dobę 7 dni w tygodniu.** Wiązać się to będzie z koniecznością wyznaczenia przez przedsiębiorcę osób pracujących w systemie pracy zmianowej i poniesienie wydatków na ten cel. **To są istotne koszty, które wpłyną na obniżenie konkurencyjności małych dostawców europejskich.**
- Rząd RP uważa, że w trakcie prac nad rozporządzeniem **należy zapewnić ochronę wolności wypowiedzi tj. zadbać by tworzone mechanizmy nie doprowadziły do zjawiska nadmiarowego usuwania treści.** Dlatego potrzebne są dodatkowe gwarancje w przypadku stosowania art. 5 rozporządzenia tj. zgłoszeń o treściach, które mogą mieć charakter terrorystyczny oraz stosowania automatycznych mechanizmów filtrowania treści terrorystycznych na podstawie art. 6.
- **W przypadku art. 5 nt. zgłoszeń problemem może być to, że w przeciwieństwie do nakazu usunięcia lub zablokowania treści, wysłanie zgłoszenia przez właściwy organ**

przerzuca ciężar oceny czy dana treść faktycznie stanowi treść o charakterze terrorystycznym z organu na dostawcę. Dostawca usług hostingowych stanie przed dylematem czy zablokować daną treść i narazić się na skargę ze strony dostawców treści (które hostingodawca ma obowiązek niezwłocznie rozpatrzeć) czy nie usuwać lub blokować treści i narazić się w takim wypadku na kary z rozporządzenia. Podobnie jest w przypadku automatycznych filtrów blokujących treści terrorystyczne.

- Zgadzamy się, że efektywne zwalczanie treści terrorystycznych w Internecie wymaga odpowiedniej współpracy pomiędzy m.in. organami ścigania i sektorem prywatnym w oparciu o jasne mechanizmy pozwalające na skuteczne realizowanie działań przez organy odpowiedzialne za zapewnienie bezpieczeństwa i porządku publicznego, przy jednoczesnym zachowaniu odpowiednich gwarancji w zakresie praw podstawowych.
- **Inną kwestią jest konieczność głębszego przeanalizowania relacji przepisów projektowanych w rozporządzeniu z Dyrektywą o handlu elektronicznym (2000/31/WE.**
- Rozporządzenie przewiduje wysokie kary i tworzy rozbudowany system nadzoru nad internetem, jednocześnie jednak jest otwarte na interpretacje i wiele kwestii pozostawia niedoprecyzowanych i niejasnych. W szczególności niejasny jest zakres przedmiotowy i podmiotowy rozporządzenia. Przykładem jest definicja dostawcy usług hostingowych, w której mieści się potencjalnie wiele podmiotów. Brakuje także precyzyjnej definicji treści terrorystycznych.

Do wiadomości Przedstawiciela Polski:

Stanowisko Rządu nie zostało jeszcze przyjęte, trwają prace nad jego przygotowaniem.

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 zawiązku 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 legislacje 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 dopływ 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[1]. 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.

[1] *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.