**PROJEKT STANOWISKA RP**

*przygotowany w związku z art. 7 ustawy z dnia 8 października 2010 r. o współpracy Rady Ministrów z Sejmem i Senatem w sprawach związanych z członkostwem Rzeczypospolitej Polskiej w Unii Europejskiej (Dz. U. Nr 213, poz. 1395)*

| | |
|---|---|
| **Dotyczy** | Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym |

| | |
|---|---|
| **Data przekazania Polsce dokumentu przez instytucje UE** | 1 października 2018 r. |

| | | |
|---|---|---|
| **Sygnatura dokumentu** | Komisja Europejska | COM(2018) 640 |
| | Numer międzyinstytucjonalny | 2018/0331 (COD) |

| | |
|---|---|
| **Procedura decyzyjna** | zwykła procedura ustawodawcza |

| | |
|---|---|
| **Tryb głosowania w Radzie UE** | |

| | |
|---|---|
| **Instytucja wiodąca** | Ministerstwo Cyfryzacji |

| | |
|---|---|
| **Instytucje współpracujące** | Ministerstwo Spraw Wewnętrznych i Administracji<br>Ministerstwo Spraw Zagranicznych<br>Ministerstwo Obrony Narodowej<br>Ministerstwo Przedsiębiorczości i Technologii<br>Ministerstwo Finansów<br>Urząd Komunikacji Elektronicznej<br>Agencja Bezpieczeństwa Wewnętrznego |

| | |
|---|---|
| **Data przyjęcia przez KSE** | 7 grudnia 2018 r. |

# I. Cel projektu aktu prawnego

**Celem rozporządzenia jest zapobieganie rozpowszechnianiu treści terrorystycznych w internecie poprzez ich jak najszybsze usuwanie i zapobieganie ponownemu umieszczeniu w sieci.**

Zgodnie z definicją treściami terrorystycznymi mogą być zarówno treści podżegające do popełnienia przestępstw terrorystycznych, pochwalające lub gloryfikujące taką aktywność, zachęcające do udziału w działalności grup terrorystycznych, jak i stanowiące instrukcje lub wskazówki dotyczące faktycznego podejmowania działań terrorystycznych.

**Zaproponowany w rozporządzeniu model opiera się na ścisłej współpracy pomiędzy właściwymi organami państwowymi, a podmiotami świadczącymi usługi hostingu**, zdefiniowanymi jako dostawcy usług społeczeństwa informacyjnego polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek oraz na udostępnianiu przechowywanych informacji osobom trzecim.

**Rozmiar ani zasięg działania dostawcy usługi nie będzie miał znaczenia dla zastosowania rozporządzenia – podobnie jak jego ewentualna lokalizacja poza obszarem Unii Europejskiej** (liczy się, że dostawca oferuje usługi w Unii Europejskiej). Rozporządzenie nie przewiduje wyłączeń dla MŚP. Zakłada się przy tym szacowanie ryzyka - część obowiązków, wynikających z projektu, ma być wykonywana w sposób proporcjonalny i odpowiedni do zidentyfikowanych ryzyk. To ma przełożyć się na zmniejszenie ciężaru regulacyjnego w przypadku mniejszych podmiotów.

**Kluczowym obowiązkiem nałożonym na dostawców usług hostingowych (art. 4) przewidzianym w projekcie jest usunięcie lub uniemożliwienie dostępu do treści terrorystycznych w ciągu jednej godziny od momentu otrzymania stosownego nakazu ze strony uprawnionego organu.** Rozporządzenie przewiduje możliwość odwołania się od takiej decyzji. Zapisane są w nim także wyjątkowe przypadki, w których jednogodzinny termin nie znajdzie zastosowania, np. w przypadku siły wyższej, lub gdy nakaz usunięcia zawiera oczywiste błędy i wymaga korekty. Co do zasady natomiast, systematyczne niedopełnianie obowiązków nakazu usunięcia (zgodnie z art. 18 ) treści może wiązać się z sankcją finansową w wysokości nawet do 4 proc. całkowitych obrotów dostawcy usług hostingowych w ostatnim roku obrotowym.

**W art. 5 przewidziano 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 decyzję, czy dany komunikat stanowi treść terrorystyczną i w zawiązku z tym powinien zostać usunięty.

**Zgodnie z art. 6 na dostawcę usługi hostingu mają zostać nałożone także obowiązki związane z proaktywnym działaniem zapobiegającym rozpowszechnianiu treści terrorystycznych.** Do takich rozwiązań zalicza się m.in. mechanizmy automatycznie analizujące treści w celu uniemożliwienia ponownego opublikowania informacji już raz usuniętych, a także wykrywania, identyfikacji i sprawnego usuwania pojawiających się nowych treści terrorystycznych. Chodzi więc o filtry blokujące publikacje treści terrorystycznych. Mechanizmy te powinny jednak działać pod nadzorem człowieka (art. 9).

Artykuł 7 rozporządzenia przewiduje przechowywanie usuniętych lub zablokowanych treści terrorystycznych. Tego typu treści powinny być przechowywane przez dostawcę usług hostingowych, z zachowaniem odpowiednich zabezpieczeń przez okres kolejnych sześciu miesięcy na potrzeby ewentualnego postępowania wyjaśniającego, prowadzonego przez właściwe organy. Te same organy będą miały również możliwość nakazania dłuższego przechowywania wspomnianych wyżej informacji.

Do dodatkowych obowiązków usługodawców świadczących usługi hostingu należeć będą również:

- Art. 8 ust. 1 - zawarcie w warunkach korzystania z usługi informacji o wdrożonej polityce zapobiegania rozpowszechnianiu treści terrorystycznych, w tym informacji o stosowanych narzędziach służących ich automatycznemu wykrywaniu.
- Art. 8 ust. 2 i 3 - sporządzanie rocznych sprawozdań dotyczących działań przedsięwziętych przez usługodawcę w zakresie przeciwdziałania terroryzmowi.
- Art. 10 przewiduje stworzenie przez hostingodawców mechanizmów rozpatrywania skarg, składanych przez dostawców treści, w przypadku usunięcia informacji terrorystycznych na skutek otrzymanego powiadomienia (w oparciu o art. 5) lub na skutek samodzielnie zastosowanych środków proaktywnych wykrywających treści o potencjalnie terrorystycznym charakterze (w oparciu o art. 6).
- Art. 11 - kontakt z dostawcami treści (których treści zostały usunięte) w zakresie podejmowanych działań, w tym w zakresie przypadków usunięcia lub uniemożliwienia dostępu do informacji publikowanych przez dostawcę treści.
- Art. 14 - powołanie punktu kontaktowego umożliwiającego odbiór nakazów usunięcia i zgłoszeń za pomocą środków elektronicznych oraz zapewniającego ich szybkie przetwarzanie na podstawie art. 4 i 5.

Do obowiązków państw członkowskich (art. 17) będzie należało wyznaczenie właściwego organu lub organów na potrzeby:

- wydawania nakazów usunięcia na podstawie art. 4.
- wykrywania, identyfikacji i zgłaszania treści o charakterze terrorystycznym dostawcom usług hostingowych na podstawie art. 5.
- nadzoru nad wdrażaniem proaktywnych środków na podstawie art. 6.
- egzekwowania obowiązków na podstawie rozporządzenia poprzez nakładanie sankcji na podstawie art. 18.
- ponadto na podstawie art. 13 państwa członkowskie powinny zapewnić koordynację i wymianę istotnych informacji - pomiędzy sobą - w odniesieniu do nakazów usunięcia i zgłoszeń. Chodzi o uniknięcie powielania działań i uniknięcia ingerencji w dochodzenia prowadzone w różnych państwach członkowskich.

## II. Stanowisko RP

**Rząd RP popiera działania służące ograniczaniu zasięgu oddziaływania propagandy terrorystycznej.** Tego rodzaju treści sprzyjają radykalizacji postaw i mogą inspirować do przygotowywania ataków, dlatego bez wątpienia są dotkliwym problemem społecznym, bez względu na skalę zjawiska w danym państwie. 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. W tym kontekście równowaga rozumiana jest jako umożliwienie skutecznego realizowania działań także przez organy odpowiedzialne za zapewnienie bezpieczeństwa i porządku publicznego, przy jednoczesnym zachowaniu odpowiednich gwarancji w zakresie praw podstawowych. Należy dodatkowo zauważyć, że oprócz treści terrorystycznych są także inne treści o charakterze nielegalnym. Dlatego nie jest wystarczająco jasne, dlaczego rozporządzenie ogranicza się jedynie do treści o charakterze terrorystycznym. Tym niemniej

**zgadzając się co do celu, jakim jest zwalczanie propagandy terrorystycznej, Rząd RP wskazuje przy tym na kwestie, które wymagają uwzględnienia podczas prac nad rozporządzeniem.**

W toku prac **należy dążyć do ograniczenia zasięgu projektowanego rozporządzenia, tak by nie obejmował on w jednakowy sposób wszystkimi przewidzianymi w nim obowiązkami małych dostawców usług hostingowych.** Przewidziane w projekcie legislacyjnym obowiązki będą łatwiejsze do spełnienia przez duże podmioty, mogą być jednak zbytnim obciążeniem finansowym dla małych i średnich dostawców rzutując na konkurencyjność świadczonych przez nich usług. Z tego też względu warto także, aby projektodawca należycie przeanalizował również skutki finansowe regulacji, w szczególności w zakresie wzrostu kosztów po stronie hostingodawców.

Rząd RP stoi na stanowisku co do konieczności **doprecyzowania zastosowanych w rozporządzeniu definicji, tak aby były one spójne z innymi aktami prawnymi i pozostawiały jak najmniejsze możliwości interpretacyjne**, które mogłyby generować problemy w momencie implementacji rozporządzenia. Jest to szczególnie istotne mając na uwadze surowość przewidzianych w projekcie rozwiązań – czy to mając na uwadze krótki czas reakcji, czy też biorąc pod uwagę dotkliwość możliwych kar finansowych. **W przypadku definicji dostawcy usług hostingowych istotnym jest jasne określenie do jakiego katalogu podmiotów odnoszą się wskazywane w nim obowiązki regulacyjne. Potrzebna jest także precyzyjna definicja treści terrorystycznych.**

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**, które nie mają charakteru propagandy terrorystycznej. Dlatego potrzebny jest mechanizm nadzoru nad wydawaniem decyzji zobowiązujących dostawców usług hostingowych do usunięcia danej treści, tak by wykluczyć przypadki bezzasadnej cenzury. Zasadne byłoby także przyznanie nieco więcej czasu na analizę zgłoszenia o usunięcie lub blokadę treści przez usługodawcę. 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. Chodzi o to aby reakcja dostawcy nie była wymuszona krótkim czasem na odpowiedź, przy jednoczesnym zagrożeniu sankcjami. Ułatwiłoby to przy tym mniejszym dostawcom możliwość bardziej elastycznego zorganizowania pracy obsługi tego typu zgłoszeń.

**Potrzebne są także gwarancje w przypadku stosowania automatycznych mechanizmów filtrowania treści terrorystycznych. Należy mieć na uwadze, że wykrywanie treści terrorystycznych to przede wszystkim zadanie dla służb państwa.** Dostawcy usług hostingowych ze swojej strony powinni zapewnić sprawną współpracę z organami państwa, nie powinni być jednak sędziami tego co jest dopuszczalne w internecie stosując własne narzędzia cenzorskie bez należytej kontroli. Zgodnie z wezwaniem Rady Europejskiej zawartym w konkluzjach z dnia 22 i 23 czerwca 2017 r. „branża w swoim własnym zakresie jest odpowiedzialna za wspieranie walki z terroryzmem i przestępczością w internecie”[1]. Dostawcy powinni mieć także możliwość odwoływania się od decyzji nakładających na nich obowiązek stosowania filtrów blokujących treści terrorystyczne do sądu. Powinna zostać także określona procedura rozpatrywania takiej skargi łącznie z ramami czasowymi przewidzianymi na jej rozpatrzenie.

**Podobnie jak w przypadku artkułu 6 należy również przeanalizować zasadność wprowadzenia w art. 5 rozporządzenia mechanizmu dotyczącego możliwości wysyłania, przez właściwy organ do dostawców usług hostingowych, zgłoszeń i dokonania głębszej refleksji odnośnie wpływu tego przepisu na wolność w internecie.** 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

[1] Posiedzenie Rady Europejskiej (22 i 23 czerwca 2017 r.) – Konkluzje (EUCO 8/17)

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 (art. 18). Trzeba przeanalizować skutki jakie pociągnie za sobą wprowadzenie zgłoszenia, czy nie spowoduje blokowania treści „na wszelki wypadek". W tym aspekcie należy się zastanowić, czy nie byłoby bardziej zasadne pozostawienie jedynie możliwości wydania sformalizowanej decyzji o nakazaniu zablokowania lub usunięcia treści – gdzie to organ sam po dokonanej analizie oraz sporządzeniu stosowanego uzasadnienia wskazywałby, które dane należy usunąć.

Rząd RP zauważa, że **w trakcie prac nad rozporządzeniem konieczne jest ustalenie relacji przepisów projektowanych w rozporządzeniu z Dyrektywą o handlu elektronicznym (2000/31/WE),** 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[2]. Artykuł 15 zakazuje państwom członkowskim nakładania na usługodawców ogólnego obowiązku monitorowania informacji.
- Art. 4 rozporządzenia zakłada usunięcie lub zablokowanie treści o charakterze terrorystycznym lub uniemożliwienie 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.

Rząd RP uważa, że **dalszych wyjaśnień, z punktu widzenia poziomu krajowego, wymaga kwestia wyznaczenia właściwych organów na potrzeby wydawania nakazów usunięcia; wykrywania, identyfikacji i zgłaszania treści o charakterze terrorystycznym; nadzoru nad wdrażaniem proaktywnych środków; egzekwowania obowiązków – nakładania sankcji.** Zgodnie z art. 17 rozporządzenia Komisja Europejska proponuje pozostawienie tej kwestii do rozstrzygnięcia państwom członkowskim. **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. Dlatego już teraz – na etapie negocjacji - należy się zastanowić, która instytucja lub instytucje w Polsce będą realizowały zadania przewidywane w rozporządzeniu. **Rozważenia wymaga, czy w ramach proponowanego wniosku nie należy zapewnić definicji organów właściwych** (pozostawiając państwom swobodę w zakresie ich wyznaczenia). Warto przy tym zwrócić uwagę, że problematykę działań antyterrorystycznych w Polsce reguluje ustawa z dnia 10 czerwca 2016 r. o działaniach

[2] *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.*

antyterrorystycznych (Dz.U. z 2018 r. poz. 452 z późn. zm.). W myśl art. 3 ust. 1 tej ustawy za zapobieganie zdarzeniom o charakterze terrorystycznym odpowiada Szef Agencji Bezpieczeństwa Wewnętrznego.

W kontekście informowania dostawców treści o usunięciu ich materiałów i ewentualnych powodach takiej decyzji, pozytywnie należy ocenić art. 11 pkt 3, który wyłącza ten obowiązek, jeżeli właściwy organ uzna, że nie powinno się ujawniać informacji ze względów bezpieczeństwa publicznego. Proponowany w art. 11 ust. 3 termin czterech tygodni wymaga dalszych analiz.

**Rząd RP pozytywnie ocenia zawartą w art. 14 propozycję ustanowienia przez dostawców usług hostingowych punktów kontaktowych umożliwiających odbiór nakazów usunięcia i zgłoszeń.** Takie podejście ułatwi kontakty organów państwa z dostawcami usług hostingu. **Pozytywnie należy ocenić także 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 wydaje się zapewnienie, aby zakres współpracy był w pełni zgodny z mandatem Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol)[3].

**Do istotnego ryzyka związanego z realizacją projektu rozporządzenia zaliczyć należy zakładane szybkie tempo wdrożenia projektowanego aktu prawnego.** W opublikowanej przez Komisję Europejską wersji dokumentu zakłada się, że rozporządzenie będzie stosowane sześć miesięcy po jego wejściu w życie. Wydaje się, że mając na uwadze konieczność dostosowania się do jego wymogów zarówno przez państwa członkowskie, jak i dostawców usług hostingowych jest to zdecydowanie zbyt krótki okres na dostosowanie się do nowych przepisów i należy go wydłużyć.

## III. Uzasadnienie stanowiska RP

Projekt rozporządzenia był przedmiotem konsultacji społecznych. Informacja w tej sprawie została zamieszczona na stronie internetowej Ministerstwa Cyfryzacji pod adresem: https://www.gov.pl/web/cyfryzacja/zapraszamy-do-konsultacji-stanowiska-rzadu-do-projektu-rozporzadzenia-w-sprawie-zapobiegania-rozpowszechnianiu-w-internecie-tresci-o-charakterze-terrorystycznym-. W toku konsultacji uwagi zgłosiły następujące podmioty:

**1. Konfederacja Lewiatan**

**Lewiatan krytycznie ocenia projekt rozporządzenia uważając, że dotychczas podejmowane działania samoregulacyjne przynoszą dobre rezultaty.**

Według Lewiatana **środki podejmowane w celu zwalczania treści terrorystycznych muszą być proporcjonalne tj. powinny uwzględniać częstotliwość występowania tego typu treści w ramach usług określonego rodzaju, a także brać pod uwagę istniejące ograniczenia techniczne.**

[3] Podstawą prawną Europolu jest *rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW*. Zgodnie z art. 23 ust. 1 ww. rozporządzenia w zakresie, w jakim jest to niezbędne do wykonywania jego zadań, Europol może ustanawiać i utrzymywać współpracę m.in. z podmiotami prywatnymi. Kwestia ewentualnych możliwości w zakresie wymiany danych osobowych z podmiotami prywatnymi jest uregulowana w artykule 26 ww. rozporządzenia.

Uwzględnienie ograniczeń technicznych jest szczególnie istotne z uwagi na przewidziane w projekcie sankcje w przypadku nie usunięcia treści terrorystycznych.

**Zaniepokojenie konfederacji budzi możliwość nałożenia na dostawców - mocą decyzji organu - usług hostingu ogólnego obowiązku monitorowania treści pod kątem treści terrorystycznych.** Stoi to w sprzeczności z art. 15 dyrektywy o handlu elektronicznym (2000/31/EC) i ratio legis tego przepisu, które mimo zmian technologicznych ciągle pozostaje aktualne.

Według Lewiatana **definicja treści terrorystycznych zawarta w rozporządzeniu jest zbyt szeroka i zbyt niejasna.** Dlatego proponuje ograniczenie zakresu rozporządzenia do treści tworzonych przez organizacje terrorystyczne znajdujące się na listach terrorystycznych UE lub ONZ, z wyłączeniem treści edukacyjnych, dokumentalnych, naukowych lub artystycznych.

Odnosząc się do art. 4 Lewiatan uważa, że **wszystkie nakazy usunięcia powinny podlegać nadzorowi sądowemu przed przesłaniem firmie**. Do tego **określenie stałych terminów (jedna godzina) na realizację tych obowiązków nie jest dobrym rozwiązaniem**. Wiążą się one ze znacznymi wyzwaniami w zakresie wdrażania oraz ryzykiem nadmiernych usunięć treści, które są sprzeczne z podstawowymi prawami obywateli w Europie. **Wymóg usunięcia treści terrorystycznych w ciągu godziny może okazać się przy tym wyzwaniem dla podmiotów o mniejszych zasobach lub w przypadku otrzymania wiadomości w dzień wolny od pracy.** W praktyce oznacza to, że każdy usługodawca będzie zobowiązany do zorganizowania dyżurów 24/7, co może być trudne przy ograniczonej liczbie pracowników. Ponieważ z uwagi na szkodliwość treści terrorystycznych wyłączenia MŚP mogłoby podważyć cel regulacji, **Lewiatan postuluje wydłużenie tego terminu, np. do 12 godzin lub posłużenie się sformułowaniem "bez zbędnej zwłoki".**

Lewiatan uważa, że **właściwe organy powinny być zobowiązane, w przypadku każdego nakazu usunięcia, do przedstawienia szczegółowego uzasadnienia takiej decyzji.** Jest to szczególnie istotne w przypadku nakazów usunięć, gdzie oczekuje się, że przedsiębiorstwa dokonają oceny w ciągu jednej godziny. Firmy, niezależnie od ich wielkości, potrzebują dokładnego wyjaśnienia, dlaczego władza uważa, że dana treść jest nielegalną treścią terrorystyczną.

Według Lewiatana obowiązki wskazane w art. 7 w zakresie przekazywania danych są nie tylko niepotrzebne, ale również mogą utrudniać realizację obowiązujących praktyk i wprowadzać konflikty prawne np. z przepisami o ochronie danych osobowych.

**Konfederacja wyraża zaniepokojenie art. 6 rozporządzenia**, które wymagałyby od dostawców usług hostingowych wdrożenia proaktywnych środków monitoringu oraz pozbawienia ich odpowiedniej ochrony (zgodnie z zasadą tzw. "dobrego samarytanina"). Może to doprowadzić do sytuacji, w której władze państw UE nakładałyby na przedsiębiorstwa określone wymogi techniczne, które są niewykonalne, niepraktyczne lub nawet przynoszą efekt przeciwny do zamierzonego. **Zdaniem Lewiatana przepisy te są niespójne z dyrektywą o handlu elektronicznym.** Ponadto, zezwolenie każdemu państwu członkowskiemu na dyktowanie konkretnego wymogu technologicznego, przy braku nadzoru ze strony Komisji Europejskiej, jest nadmierne i jednocześnie może prowadzić do **cenzury i fragmentacji rynku cyfrowego** w Europie.

W odniesieniu do sankcji przewidzianych w rozporządzeniu Konfederacja wyraża obawę, że ograniczą one podstawowe prawa Europejczyków. Wysokie grzywny i krótkie terminy doprowadzą do błędnych decyzji i stworzą zachęty do nadgorliwych usunięć, które mogą doprowadzić do efektu mrożącego (chilling effect) w odniesieniu do praw podstawowych. Ponadto przepisy dotyczące sankcji są wg. Lewiatana źle zdefiniowane i będą prowadzić do zróżnicowania kar w poszczególnych państwach członkowskich. Lepszym rozwiązaniem byłoby, gdyby jedyny właściwy organ działający w imieniu UE-27 mógł nakładać proporcjonalne do naruszenia kary. Przepisy wymagają także uzupełnienia o

obowiązek zagwarantowania usługodawcy prawa do odwołania się od decyzji organu nakładającego sankcję.

Konfederacja uważa, że usługi hostingowe powinny być chronione przed odpowiedzialnością, gdy podejmują proaktywne działania w celu identyfikacji szkodliwych treści ("dobry samarytanin"). Zasada 'dobrego samarytanina' nie powinna prowadzić do uznania, że usługodawca hostingowy ponosi odpowiedzialności za informacje, które udostępnia tylko dlatego, że podjął dobrowolne działanie w dobrej wierze, zarówno o charakterze automatycznym, jak i niezautomatyzowanym.

**2. Związek Pracodawców Branży Internetowej - Interactive Advertising Bureau (IAB Polska)**

**IAB wskazuje na duże i kosztowne zmiany organizacyjne, które będą się wiązały z realizacją rozporządzenia po stronie dostawców usług hostingowych. Krytykuje także niejasność proponowanych środków.** Izba wskazuje, że rozporządzenie będzie miało zastosowanie zarówno do dużych, jak i małych platform, także i tych na których treści terrorystyczne nie występują lub występują sporadycznie. Całokształt regulacji będzie prowadził do nałożenia na dostawców usług hostingowych odczuwalnych kosztów realizacji obowiązków, na które nie mogą pozwolić sobie mniejsze podmioty. **W ocenie IAB Polska może to odbić się na rozwoju całej branży usług społeczeństwa informacyjnego.** Dlatego w ocenie IAB Polska zasadne są m.in. dalsze prace nad definicją dostawcy usług hostingowych tak, aby ograniczyć krąg podmiotów mogących się do niej kwalifikować.

**Izba zauważa, że proponowane przez projekt rozporządzenia rozwiązania stanowią wyraźne odstępstwo od art. 15 dyrektywy o handlu elektronicznym**, który zakłada nienakładanie na usługodawców ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność.

**Wymóg usunięcia treści terrorystycznych w ciągu godziny będzie według Izby zachęcał do automatycznego usuwania treści, nawet w razie wątpliwości co do tego, czy treści propagują terroryzm, co negatywnie odbije się na użytkownikach portali.** Do automatycznego usuwania treści „zachęcać" będą również surowe kary finansowe, jakie mogą być nałożone dostawcę usług hostingowych. W związku z powyższym **dla IAB absolutnym minimum zmian w rozporządzeniu powinno być wydłużenie tego czasu do przynajmniej 12 godzin.**

Odnosząc się do art. 6 IAB niepokoi wprowadzony mechanizm zgodnie z którym, gdy upoważniony organ uzna niewystarczające do ograniczenia ryzyka i poziomu narażenia oraz do zarządzania tym ryzykiem i poziomem narażenia, może zażądać od dostawcy usług hostingowych wprowadzenia dodatkowych szczególnych proaktywnych środków. Dlatego **IAB chciałoby jasnych ram czasowych w procedurze odwoławczej od decyzji o konieczności wprowadzenia mechanizmów filtrowania treści, a także odpowiedniej kontroli sądowej decyzji wydawanych przez upoważniony organ.**

W ocenie IAB Polska szczególnie cenne w perspektywie wymogów dot. przejrzystości (art. 8 rozporządzenia) byłoby opracowanie jednolitego stałego szablonu sprawozdania, który umożliwiłoby jednorazowe przygotowanie systemów raportowych usługodawców do określonych wymogów cyklicznej sprawozdawczości.

**3. Google**

**Firma krytykuje definicje dostawców usług hostingowych** z uwagi na niejasność i fakt, że jest niezgodna z terminologią przyjętą w dyrektywie o handlu elektronicznym. **Zwraca dodatkowo uwagę na ryzyko, że wyszukiwarki będą traktowane w podobny sposób jak platformy hostingowe**, choć wyszukiwanie jest zasadniczo różne od hostowania i nawet działania przez wyszukiwarki nie sprawiają, że treści znikają z sieci.

**Wskazuje, że, projekt sam w sobie jest niespójny pod względem terminologii. Google zwraca uwagę, że obciążeniami regulacyjnymi będą objęte także małe firmy.** Wskazuje także, że firma podejmuje już teraz działania na rzecz zwalczania nielegalnych treści.

**4. Fundacja Panoptykon**

Fundacja poddaje w wątpliwość, czy rozporządzenie jest w ogóle potrzebne. **Krytykuje Komisję Europejską za brak pogłębionej analizy potrzeby przyjęcia nowego aktu prawnego i brak wyliczenia kosztów wdrożenia przewidzianych w projekcie rozwiązań.**

W dalszej części stanowiska Fundacja wskazuje na **nieprecyzyjny charakter definicji treści o charakterze terrorystycznym, który stwarza zagrożenie usuwania treści, których dostępność nie stwarza realnego (lub zgoła żadnego) zagrożenia**. Szczególnie istotny jest brak kryterium zagrożenia wiążącego się z dostępnością określonej treści.

**Fundacja krytykuje dopuszczenie możliwości przeciwdziałania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym w formie nieformalnego zgłoszenia – na podstawie art. 5 rozporządzenia.** Propozycja legislacyjna pozostawia swobodę właściwym krajowym organom w wyborze ścieżki działania. Fundacja przypuszcza, że wybierana będzie ta „wygodniejsza", to jest zgłoszenia. Tryb ten nie zawiera jednak wystarczających gwarancji dla dostawców treści, a jednocześnie stanowi rezygnację organów państwa na rzecz prywatnych podmiotów z realizacji zadań w zakresie przeciwdziałania terroryzmowi. Stawia on hostingodawców w roli arbitrów rozstrzygających ostatecznie o dopuszczalności danej treści w sieci, pomimo, że podmioty te mają znacznie bardziej ograniczone kompetencje do rzetelnej analizy zgłaszanych materiałów. **Stanowi to według Panoptykonu przejaw prywatyzacji walki z terroryzmem, która to walka należy do zadań państwa i odpowiedzialność za nią nie powinna być w żadnej mierze delegowana na podmioty prywatne. Dlatego fundacja postuluje rezygnację z „trybu niewiążącego" i wprowadzenie jednolitego obligatoryjnego trybu usuwania bądź blokowania treści o charakterze terrorystycznym przez dostawców usług internetowych, na żądanie uprawnionego organu.**

**Dla Panoptykonu kluczowe jest, aby zaangażowanie organów państwa w blokowanie bądź usuwanie treści w Internecie opierało się na jasnej, odpowiedzialnej i podlegającej skutecznej weryfikacji ocenie danego materiału w oparciu o przepisy powszechnie obowiązującego prawa.** W zakresie trybu podejmowania decyzji o nakazie usunięcia treści (art. 4 rozporządzenia) – projekt powinien wprowadzać standard analogiczny do standardu przewidzianego w art. 32c polskiej ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Wiążący nakaz powinien być wydawany przez niezależny sąd. W związku z tym art. 12 projektu powinien nałożyć na państwa członkowskie obowiązek, by właściwe organy, o których mowa w art. 17 pkt 1 lit. a) nie tylko dysponowały niezbędnymi zdolnościami i wystarczającymi zasobami do realizacji rozporządzenia, ale były także organami niezależnymi od władzy wykonawczej.

Oceniając art. 6 Fundacja postuluje stworzenie mechanizmu skargi dostępnego dla dostawców zablokowanej/usuniętej treści w wyniku stosowania środków proaktywnych (i każdej decyzji podejmowanej w oparciu o wewnętrzne regulacje). Mechanizm ten nie powinien ograniczać się do wewnętrznej procedury odwoławczej, ale obejmować także możliwość odwołania się, od ostatecznej decyzji dostawców usług hostingowych, do sądu. Rozporządzenie powinno także przewidywać możliwość zaskarżenia przez hostingodawcę decyzji organu nadzorującego o nałożeniu obowiązku stosowania proaktywnych środków przed sądem.

**1. Ocena skutków prawnych**

Rozporządzenie będzie wymagało dostosowań w prawie krajowym. W szczególności zadaniem państwa będzie wyznaczenie organów właściwych odpowiadających za realizację zadań wynikających z przyjętych przepisów. Wskazując na dotychczasowe rozwiązania przyjęte na poziomie krajowym w zakresie przeciwdziałania rozpowszechnianiu treści o charakterze terrorystycznym w Internecie, należy wspomnieć, że zostały one wprowadzone ustawą z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych. Zgodnie z dodanym w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu art. 32c ust. 1 w celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym oraz ścigania ich sprawców sąd, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, w drodze postanowienia, może zarządzić zablokowanie przez usługodawcę świadczącego usługi drogą elektroniczną dostępności w systemie teleinformatycznym określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym. W przypadkach niecierpiących zwłoki, jeżeli mogłaby ona spowodować zdarzenie o charakterze terrorystycznym, Szef ABW, po uzyskaniu pisemnej zgody Prokuratora Generalnego, może zarządzić blokadę dostępności, zwracając się jednocześnie do Sądu Okręgowego w Warszawie z wnioskiem o wydanie postanowienia w tej sprawie (art. 32c ust. 4). Usługodawca świadczący usługi drogą elektroniczną jest obowiązany do natychmiastowego dokonania czynności określonych w postanowieniu sądu lub przekazanym mu żądaniu Szefa ABW (art. 32c ust. 5). Zgodnie z art. 32c ust. 7 blokadę dostępności zarządza się na okres nie dłuższy niż 30 dni. Sąd Okręgowy w Warszawie może, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, wydać postanowienie o jednorazowym przedłużeniu blokady dostępności na okres nie dłuższy niż 3 miesiące, jeżeli nie ustały przyczyny jej zarządzenia. Sposób dokumentowania blokady dostępności oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków określony został w rozporządzeniu Prezesa Rady Ministrów z dnia 18 lipca 2016 r. w sprawie sposobu dokumentowania blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków.

**2. Ocena skutków społecznych**

Rozporządzenie daje dodatkowe narzędzia służące zmniejszeniu oddziaływania propagandy terrorystycznej na społeczeństwo. Blokowanie treści terrorystycznych i ich szybsze usuwanie to zmniejszenie ryzyka zetknięcia się z treściami terrorystycznymi w internecie. Jednocześnie istnieje ryzyko nadmiarowego usuwania treści przez dostawców usług hostingowych, odgraniczając tym samym swobodę wypowiedzi.

**3. Ocena skutków gospodarczych**

Rozpatrując projekt 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.

**4. Ocena skutków finansowych**

W związku z przyjęciem aktu prawnego mogą pojawić się umiarkowane koszty dla państw członkowskich w tym dla Polski. Jednocześnie bardzo trudno będzie wskazać skutki finansowe dla Polski. Wydatki wiążą się z kosztem wdrożenia i utrzymania systemu egzekwowania przewidywanych w rozporządzeniu obowiązków regulacyjnych nakładanych na dostawców usług hostingowych. Po stronie państw członkowskich będzie leżał (wskazany art. 17 rozporządzenia) obowiązek wyznaczenia organów właściwych do egzekwowania poszczególnych przepisów.

Rząd RP będzie miał na uwadze konieczność przyjęcia takich uregulowań, które nie będą powodować nadmiernego zwiększenia kosztów po stronie budżetu państwa. Ewentualne koszty po stronie budżetu państwa potrzebne do realizacji zadań związanych z wprowadzeniem nowych rozwiązań, zostaną sfinansowane w ramach corocznie ustalanego w ustawie budżetowej limitu wydatków we właściwej części budżetowej i nie będą stanowiły podstawy do ubiegania się o dodatkowe środki z budżetu państwa na ten cel w roku bieżącym, jak i w kolejnych latach budżetowych.

## IV. Informacja w sprawie zgodności projektu aktu z zasadą pomocniczości

Rząd RP stoi na stanowisku, że inicjatywa legislacyjna jest zgodna z zasadą pomocniczości.

## V. Przedstawiciel Rządu upoważniony do prezentowania stanowiska

Pani Wanda Buk, podsekretarz stanu, Ministerstwo Cyfryzacji