Warszawa, 26 kwietnia 2024 roku

Szanowny Pan Jurand Drop
Sekretarz Stanu
Ministerstwo Spraw Wewnętrznych i Administracji
dep.prawny@mswia.gov.pl

do wiadomości:
Szanowny Pan Krzysztof Gawkowski
Wicepremier, Minister Cyfryzacji
i Pełnomocnik Rządu ds. Cyberbezpieczeństwa
sekretariat.drc@mc.gov.pl

STANOWISKO POLSKIEJ IZBY KOMUNIKACJI ELEKTRONICZNEJ
w przedmiocie projektu ustawy o zmianie ustawy o działaniach antyterrorystycznych oraz ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (UD37)

Szanowny Panie Ministrze,

dnia 19 kwietnia 2024 roku w Biuletynie Informacji Publicznej na stronie Rządowego Centrum Legislacji został opublikowany **projekt ustawy o zmianie ustawy o działaniach antyterrorystycznych oraz ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu** (UD37, dalej „projekt ustawy"). Uzasadnieniem projektu ustawy jest implementacja do polskiego porządku prawnego rozporządzenia Parlamentu Europejskiego i Rady UE 2021/784 z dnia 29 kwietnia 2021 roku w sprawie przeciwdziałania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym (dalej „rozporządzenie UE").

Rozporządzenie UE podobnie jak art. 1 projektu ustawy konkretyzują obowiązki na dostawców treści i usług hostingowych w zakresie usuwania lub blokowania treści określonych jako terrorystyczne.

Niestety w art. 2 projektu ustawy wprowadza zmianę w art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, gdzie wskazuje, że na przedsiębiorców telekomunikacyjnych (a nie na dostawców usług hostingowych jak obecnie) mogą być nałożone obowiązki *„usunięcia lub zablokowania dostępności w systemie teleinformatycznym określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze*

terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa". W uzasadnieniu projektu ustawy wyjaśnia się, że jest to konieczne z powodu poprawnej implementacji art. 21 dyrektywy 2017/541 z dnia 15 marca 2017 roku w sprawie zwalczania terroryzmu i zastępującej decyzję ramową Rady 2002/475/WSiSW oraz zmieniającej decyzję Rady 2005/671/WSiSW.

PIKE wskazuje, że proponowana zmiana art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu **jest błędna**. Po pierwsze, zmienia ona podmioty zobowiązane do wykonania obowiązków „*usunięcia lub blokady dostępu*" z dostawców usług świadczonych elektronicznie na przedsiębiorców telekomunikacyjnych.

Izba wskazuje, że obecne brzmienie tego przepisu jest prawidłowe, jeśli chodzi o możliwości techniczne, prawne i organizacyjne zobowiązanego podmiotu. Należy podkreślić, że dostawcy usług hostingowych mają możliwość usunięcia z zarządzanych przez siebie systemów teleinformatycznych określonych treści lub zablokowanie dostępu do nich, **których to możliwości nie mają że przedsiębiorcy telekomunikacyjni**. Zwracamy przy tym uwagę, że przywołana w uzasadnieniu projektu ustawy unijna dyrektywa nie wskazuje, że podmiotem usuwającym dane treści z sieci Internet mają być przedsiębiorcy telekomunikacyjni.

W opinii PIKE, art. 2 projektu ustawy w proponowanym kształcie jest obecnie **niewykonalny, sprzeczny z polskimi i unijnymi przepisami, a także niepotrzebny.**

W zakresie obowiązku „*usuwania*" podkreślamy, że przedsiębiorcy telekomunikacyjni **nie mają możliwości usuwania jakichkolwiek treści** w systemie teleinformatycznym innych podmiotów. Przedsiębiorca telekomunikacyjny zapewnia jedynie dostęp swoim użytkownikom do usługi szerokopasmowego dostępu do Internetu, bez jakiegokolwiek wpływu na dostępne w niej treści innych podmiotów (m.in. dostawców usług drogą elektroniczną, w tym dostawców usług hostingowych). Z tego względu przedsiębiorca telekomunikacyjny nie ma dostępu do systemów umożliwiających mu modyfikowanie *określonych danych informatycznych* (może jedynie przesyłać te dane od i do abonenta w formie zakodowanej). W tym zakresie należy zwrócić uwagę na treść art. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiającego środki dotyczące dostępu do otwartego Internetu oraz zmieniającego dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenia (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii (Dz. Urz. UE. L. 2015.310.1 z późn. zm. dalej „Rozporządzenie o otwartym Internecie"). W art. 3 ust. 3 Rozporządzenia o otwartym Internecie jest mowa o uprawnieniach dostawców dostępu do sieci Internet w zakresie zarządzania ruchem, bez możliwości monitorowania przez nich konkretnych treści. Przedsiębiorca telekomunikacyjny może więc jedynie w wąskim zakresie zarządzać ruchem w zakresie dostępu do treści w sieci Internet, ale nie może w nie ingerować czy też je monitorować. Na tej prawnej regulacji opierają się techniczne zasady świadczenia usługi dostępu do sieci Internet.

Równie dużym problemem jest nałożenie na przedsiębiorców telekomunikacyjnych obowiązku „*blokowania dostępu*”. Jak już wskazano wcześniej, zgodnie z art. 3 ust. 3 rozporządzenia o otwartym Internecie, przedsiębiorca telekomunikacyjny może w wąskim zakresie blokować dostęp do treści, ale bez możliwości ich monitorowania. Treść projektu ustawy nie konkretyzuje kwestii technicznych tego obowiązku, co jest kluczowe dla jego realizacji. Izba podkreśla, że przedsiębiorca telekomunikacyjny nie ma możliwości blokowania dostępu do wskazanych treści, ale ma możliwości **blokowania dostępu do domeny internetowej**, na której są zakazane treści.

Izba pragnie zwrócić uwagę, iż jej stanowisko opiera się na rozumieniu zasad i zakresu przedmiotowego rozporządzenia o otwartym Internecie oraz stanowiska BEREC w tejże kwestii, w szczególności przedstawionym w dokumencie *"An assessment of IP interconnection in the context of Net Neutrality"*[1], gdzie BEREC opisuje zakres usługowy dostawców dostępu do Internetu, oraz dostawców treści i aplikacji (strona 5 dokumentu BEREC). Schemat ten wyraźnie wskazuje, że zakres odpowiedzialności usługowej dostawcy dostępu do sieci Internet ogranicza się do kwestii fizycznej sieci, a nie treści czy aplikacji w Internecie.

Przyjęta w Polsce zasada wyjątkowego blokowania treści w Internecie (w oparciu o usługi DNS świadczone przez dostawców dostępu do sieci Internet) jest związana w wspomnianym już art. 3 ust. 3 rozporządzenia o otwartym Internecie, gdzie zakazuje się przedsiębiorcom telekomunikacyjnym monitorowania treści przesyłanych i odbieranych przez ich abonentów. Stosowane w Polsce blokowanie domen internetowych na poziomie DNS pozwala na blokowanie określonych treści bez konieczności monitorowania przesyłanych danych i bez naruszania przepisów rozporządzenia o otwartym Internecie. Podkreślamy, że z powodów prawych i technicznych żadna sieć telekomunikacyjna w Polsce nie może być przystosowana do monitorowania i blokowania określonych treści.

Powyżej omówione rozwiązanie zostało przyjęte w ustawie o grach hazardowych oraz w ustawie o zwalczaniu nadużyć w komunikacji elektronicznej, a także implementacja tożsamego rozwiązania planowana jest również w projekcie ustawy o kryptoaktywach. Realizacja postanowień art. 15f ust. 5. ustawy o grach hazardowych, jednoznacznie i w sposób nie pozostawiający żadnej swobody interpretacji mówi o obowiązku „*uniemożliwienia dostępu do stron internetowych wykorzystujących nazwy domen internetowych wpisanych do Rejestru prowadzonego przez Ministerstwo Finansów poprzez ich usunięcie z systemów teleinformatycznych przedsiębiorców telekomunikacyjnych, służących do zamiany nazw domen internetowych na adresy IP*". Takie działanie dotyczy wyłącznie usługi tłumaczenia adresów, w żaden sposób nie wpływa na ruch internetowy, który może wygenerować Abonent.

Należy zaznaczyć, iż kwestia usuwania i blokowania treści przez przedsiębiorców telekomunikacyjnych była już przedmiotem dyskusji na forum Sejmu w 2023 roku przy okazji

[1] https://www.berec.europa.eu/sites/default/files/files/news/bor_12_33_ip_ic_assessment.pdf

procedowania projektu ustawy o ochronie małoletnich przed dostępem do treści nieodpowiednich w Internecie (UD451).

Jednocześnie PIKE podkreśla, że art. 21 dyrektywy 2017/541 z dnia 15 marca 2017 roku w sprawie zwalczania terroryzmu i zastępujący decyzję ramową Rady 2002/475/WSiSW oraz zmieniający decyzję Rady 2005/671/WSiSW, został już implementowany do polskiego porządku prawnego w **art. 180 ustawy Prawo telekomunikacyjne**, a także był wykorzystywany przez ABW w roku 2022 do blokowania rosyjskiej propagandy (zablokowano wówczas domenę internetową programu w Wrealu24 i wiele innych). Przepis ten jest również transponowany do projektowanego właśnie Prawa komunikacji elektronicznej (art. 53). W obu tych przypadkach blokowanie dotyczy domen internetowych, a nie treści czy wskazanych danych i odbywa się z pomocą ekspertów Urzędu Komunikacji Elektronicznej.

Co więcej, kwestiami usuwania i blokowania dostępu do określonych treści zajmuje się również rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych DSA). Izba wskazuje, że DSA wyraźnie rozdziela obowiązki dostawców usług bezpośrednich w zakresie treści w sieci Internet, podkreślając rolę dostawców usług hostingowych w zakresie usuwania i blokowania treści nielegalnych (w tym o charakterze terrorystycznych). Co więcej, DSA wskazuje, że zaufanym podmiotem zgłaszającym nielegalne treści mogą być organy ścigania, a takie zgłoszenie może być podstawą do wydania nakazu określonego działania.

Podsumowując, PIKE **postuluje usunięcie z projektu ustawy art. 2 zmieniającego art. 32c** ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, jako wykraczającego poza przepisy unijne jakie projekt ustawy ma wdrożyć, a także jako wadliwego i sprzecznego z przepisami telekomunikacyjnymi.

Ponadto wnosimy, aby wszelkie prace legislacyjne związane z usuwaniem treści w Internecie lub blokowaniem dostępu do nich odbywały się z udziałem **ekspertów CSIRT NASK, głównego ośrodka cyberbezpieczeństwa w Polsce,** a także przedstawicieli Urzędu Komunikacji Elektronicznej oraz izb skupiających przedsiębiorców telekomunikacyjnych. Pozwoli to na wypracowanie spójnej rządowej strategii w zakresie zwalczania niebezpiecznych treści w sieci Internet oraz wdrożenie najlepszych mechanizmów służących realizacji tych działań.

Z wyrazami szacunku,

B. Łaga

Bogdan Łaga
Prezes Zarządu
Polska Izba Komunikacji Elektronicznej