UZASADNIENIE

W związku z wejściem w życie z dniem 7 czerwca 2021 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79), zwanego dalej „rozporządzeniem 2021/784”, zaistniała potrzeba zainicjowania prac legislacyjnych mających na celu dostosowanie polskiego porządku prawnego do uregulowań unijnych. Państwa członkowskie, w tym Polska, są zobowiązane do odpowiedniego dostosowania swoich regulacji i stosowania rozporządzenia 2021/784, począwszy od dnia 7 czerwca 2022 r. Projekt ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu wprowadza do polskiego porządku prawnego stosowne przepisy, które to umożliwią.

Głównym motywem wydania rozporządzenia 2021/784 było zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego przez przeciwdziałanie wykorzystywaniu usług hostingowych do celów terrorystycznych oraz przyczynianie się do poprawy bezpieczeństwa publicznego w całej Unii Europejskiej, przy jednoczesnym zagwarantowaniu pełnego poszanowania praw podstawowych, takich jak wolność wypowiedzi i informacji. Nowe uregulowania – co do zasady – ustanawiają we wszystkich państwach członkowskich UE spójny mechanizm umożliwiający skuteczne i legalne usuwanie z sieci oraz blokowanie wszelkich treści o charakterze terrorystycznym zamieszczanych z wykorzystywaniem usług hostingowych. Mając na uwadze transgraniczny charakter problemu oraz fakt, że treści o charakterze terrorystycznym są często publicznie rozpowszechniane za pośrednictwem usług świadczonych przez zagranicznych dostawców usług hostingowych, mechanizm ten ma zastosowanie wobec wszystkich dostawców, niezależnie od miejsca ustanowienia ich głównej jednostki organizacyjnej, jeżeli swoje usługi oferują w co najmniej jednym państwie członkowskim UE. W tym zakresie obowiązuje zasada równego traktowania, a działania podejmowane w celu stosowania przyjętych rozwiązań muszą być skuteczne, odpowiednie i proporcjonalne. Środki służące przeciwdziałaniu rozpowszechniania w internecie treści o charakterze terrorystycznym, w rozumieniu projektowanej regulacji, w przypadku gdy pozostają skuteczne i proporcjonalne, nie są sprzeczne z ochroną wolności wypowiedzi i informacji, lecz ochronę tę wzmacniają, przede wszystkim zapewniając bezpieczeństwo mediów cyfrowych przed działaniami grup terrorystycznych i ich zwolennikami.

Komisja Europejska, powołując się na dane Europolu, wskazuje na rosnące zainteresowanie wykorzystaniem internetu przez terrorystów, m.in. do szerzenia swoich przesłań w celu zastraszania, radykalizacji, rekrutacji oraz ułatwiania przeprowadzania ataków terrorystycznych. W ocenie Komisji Europejskiej jest to szczególnie niebezpieczne w aktualnej sytuacji geopolitycznej w kontekście panujących konfliktów i niestabilności, które mają bezpośredni wpływ na bezpieczeństwo Europy. Jak wskazuje Komisja Europejska, cyt. „Rosyjska wojna napastnicza przeciwko Ukrainie i atak terrorystyczny przeprowadzony przez Hamas na Izrael 7 października 2023 r. doprowadziły do zwiększenia skali rozpowszechniania w internecie treści o charakterze terrorystycznym.”[[1]](#footnote-1)).

W świetle rozporządzenia 2021/784 za treści o charakterze terrorystycznym należy uznać materiały, które:

* podżegają do popełnienia przestępstwa terrorystycznego (w rozumieniu dyrektywy 2017/541 z dnia 15 marca 2017 r.[[2]](#footnote-2))), w przypadku gdy takie materiały bezpośrednio lub pośrednio (np. przez pochwalanie aktów terrorystycznych) popierają popełnianie przestępstwa terrorystycznego, a tym samym stwarzają niebezpieczeństwo popełnienia jednego lub większej liczby takich przestępstw,
* nakłaniają osobę lub grupę osób do popełnienia lub przyczynienia się do popełnienia przestępstwa terrorystycznego,
* nakłaniają osobę lub grupę osób do uczestniczenia w działaniach grupy terrorystycznej,
* udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji lub w zakresie innych szczególnych metod lub technik w celu popełnienia lub przyczynienia się do popełnienia przestępstwa terrorystycznego;
* stwarzają zagrożenie popełnienia przestępstwa terrorystycznego.

Treściami o charakterze terrorystycznym w rozumieniu rozporządzenia 2021/784 nie są natomiast materiały rozpowszechniane w celach: edukacyjnych, dziennikarskich, artystycznych, badawczych czy zwiększania świadomości na temat przeciwdziałania działalności terrorystycznej. Treściami o charakterze terrorystycznym nie powinny być również wyrażane w ramach debaty publicznej radykalne, polemiczne lub kontrowersyjne poglądy na drażliwe kwestie polityczne. Przepisy rozporządzenia 2021/784 nie będą miały także zastosowania wobec usług poczty elektronicznej lub przesyłanych wiadomości prywatnych, a także do infrastruktury w chmurze, pod warunkiem że usługi te są świadczone na wniosek stron innych niż dostawcy treści i przynoszą korzyści dostawcom treści jedynie pośrednio. Natomiast rozporządzenie 2021/784 stosuje się do dostawców usług w zakresie mediów społecznościowych, usług wymiany materiałów video, obrazów i plików audio, a także usług wymiany plików i innych usług w chmurze, jeżeli usługi te są wykorzystywane do publicznego udostępnienia przechowywanych informacji na bezpośredni wniosek dostawcy treści.

W rezultacie państwa członkowskie zostały zobowiązane do wskazania w swoich porządkach prawnych takich organów, które bez względu na skalę zjawiska w danym państwie będą w stanie sprawnie i skutecznie zapewnić ochronę przed internetową propagandą terrorystyczną, mając przy tym do dyspozycji niezbędne do tego narzędzia zarówno na poziomie operacyjnym, jak i prawno-administracyjnym.

Zgodnie z internetowym rejestrem zawierającym wykaz takich organów obowiązek ten wypełniły 24 państwa, które tym samym zapewniły możliwość stosowania rozporządzenia[[3]](#footnote-3)). Z opublikowanego w 2024 r. przez Komisję Europejską raportu wynika, że do 31 grudnia 2023 r. Komisja Europejska otrzymała informację o co najmniej 349 nakazach usunięcia wysłanych przez właściwe organy Hiszpanii, Rumunii, Francji, Niemiec, Austrii i Czech m.in. do następujących podmiotów: Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L., FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net oraz Catbox. Przy czym hiszpański organ właściwy wysłał 62 nakazy, francuski 26 nakazów, natomiast tylko od czasu ataku terrorystycznego przeprowadzonego przez Hamas na Izrael w październiku 2023 r. do końca 2023 r. niemiecki organ takich nakazów wysłał blisko 250[[4]](#footnote-4)).

Jednocześnie tylko w dziesięciu przypadkach dostawca usług hostingowych nie usunął treści o charakterze terrorystycznym lub nie zablokował dostępu do nich w czasie do jednej godziny, do czego zobowiązuje rozporządzenie 2021/784. W efekcie dzięki wdrożonym mechanizmom bardzo wzrosła szybkość reagowania na zgłoszenia dotyczące takich treści. W dziewięciu przypadkach EUROPOL otrzymał od dostawców usług hostingowych informacje na temat treści o charakterze terrorystycznym, które wiązały się z bezpośrednim zagrożeniem życia, zgodnie z art. 14 ust. 5 rozporządzenia[[5]](#footnote-5)).

Tematyka rozporządzenia 2021/784 obecnie jest częściowo objęta regulacją krajową, która nie w pełni wdraża obowiązującą w tym zakresie dyrektywę Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW, zwaną dalej „dyrektywą 2017/541”.

W świetle ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu , zwanej dalej „ustawą o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu”, Szef Agencji Bezpieczeństwa Wewnętrznego, za zgodą sądu, może spowodować tzw. „blokadę dostępności” w internecie określonych danych powiązanych ze zdarzeniem o charakterze terrorystycznym. Zgodnie z art. 32c ww. ustawy, sąd, na pisemny wniosek Szefa ABW złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, w drodze postanowienia, może zarządzić zablokowanie dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa. Zaś w przypadkach niecierpiących zwłoki do zarządzenia takiej blokady uprawniony jest Szef ABW, po uzyskaniu pisemnej zgody od Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego. Jednocześnie w takiej sytuacji Szef ABW jest zobowiązany zwrócić się do Sądu Okręgowego w Warszawie z pisemnym wnioskiem o wydanie postanowienia w przedmiotowej sprawie. W przypadku gdy sąd w terminie 5 dni nie udzieli zgody na zarządzenie blokady, jest ona znoszona. W pozostałych przypadkach blokada dostępności danych teleinformatycznych jest zarządzana na okres nie dłuższy niż 30 dni z możliwością jej sądowego przedłużenia na okres nie dłuższy niż 3 miesiące.

Z kolei zgodnie z art. 21 dyrektywy 2017/541 państwa członkowskie są zobowiązane do wprowadzenia środków, które w pierwszej kolejności zapewnią natychmiastowe usunięcie treści internetowych nawołujących do popełnienia przestępstwa terrorystycznego. Natomiast jeżeli usunięcie takich treści nie jest możliwe, państwa członkowskie mogą podjąć środki w celu zablokowania dostępu do nich. Polskie ustawodawstwo zaś przewiduje jedynie możliwość zablokowania odpowiednich treści, co w ocenie Komisji Europejskiej nie jest wystarczające, aby uznać transpozycję przepisów dyrektywy 2017/541 w tym zakresie za prawidłową. Brak jest bowiem podstawowego mechanizmu, który pozwalałby w pierwszej kolejności na usuwanie tych treści ze stron internetowych.

Projektując obowiązujące w tym zakresie rozwiązania krajowe, przyjęte ustawą z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych , zwaną dalej „ustawą o działaniach antyterrorystycznych”, wzorowano się na wówczas już funkcjonujących przepisach dotyczących zarządzania kontroli operacyjnej w poszczególnych służbach. Ogólnie wynika z nich, że blokada treści o charakterze terrorystycznym w internecie wymaga – co do zasady – uprzedniej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego i sądu.

Z kolei mechanizm ustanowiony w rozporządzeniu 2021/784 jest znacznie szybszy i uproszczony. Unijne regulacje nie zakładają konieczności uzyskania sądowej zgody do jego zastosowania. Natomiast zapewniają wdrożenie procedury skargowej, do której będzie miała prawo każda ze stron, której wydany nakaz dotyczy, tj. zarówno dostawcy usług hostingowych, jak i dostawcy treści, które zostały usunięte.

W związku z tym jest konieczne dokonanie stosownej nowelizacji ustawy o działaniach antyterrorystycznych, która spowoduje, że również Polska znajdzie się w grupie państw członkowskich, które dysponują zwiększonym potencjałem zarówno w sferze prawnej, jak i funkcjonalnej w walce przeciwko wykorzystywaniu internetu do działań terrorystycznych. Obecnie, jak przedstawiono powyżej, aktualny stan prawny nie tylko nie przewiduje możliwości usuwania przez służby niebezpiecznych treści terrorystycznych ze stron internetowych, ale – co za tym idzie – nie pozwala na korzystanie z ustanowionych w tym celu narzędzi rynku cyfrowego. Należy wskazać, że od 3 lipca 2023 r. funkcjonuje opracowana przez EUROPOL platforma o nazwie „PERCI”, która centralizuje, koordynuje i ułatwia przekazywanie nakazów usunięcia i zgłoszeń do dostawców usług hostingowych. Jest to rozwiązanie oparte na chmurze zapewniające bezpieczeństwo i ochronę danych zamieszczanych w chmurze. Obecnie oprócz roli, jaką pełni w odniesieniu do zgłoszeń, PERCI ułatwia przekazywanie nakazów usunięcia, sprawozdawczość państw członkowskich i koordynację, a także usuwanie konfliktów, w sytuacji gdy toczy się postępowanie przygotowawcze w sprawie treści, wobec których ma zostać wysłany nakaz usunięcia. Równocześnie trwają dalsze prace w kierunku wykorzystania tego systemu do realizacji kolejnych zadań wynikających z rozporządzenia 2021/784, np. weryfikacji transgranicznych nakazów usunięcia.

Mając powyższe na uwadze, niniejszym projektem proponuje się wprowadzenie zmian do ustawy o działaniach antyterrorystycznych przez dodanie do słownika ustawy definicji pojęć: „dostawcy usług hostingowych”, „dostawcy treści” oraz „treści o charakterze terrorystycznym” przez odesłanie do odpowiednich definicji zawartych w rozporządzeniu 2021/784 (art. 1 pkt 1 projektu). W obecnym brzmieniu ustawy o działaniach antyterrorystycznychpojęcia te nie występują, w związku z tym ich wprowadzenie na grunt ustawowy wymaga odesłania w tym zakresie do przepisów prawa unijnego. Jest to niezbędne celem zapewnienia prawidłowego stosowania i jednolitego interpretowania projektowanych przepisów dotyczących przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym.

W rezultacie zgodnie z niniejszym projektem „treści o charakterze terrorystycznym” to materiały, które:

1. podżegają do popełnienia przestępstwa o charakterze terrorystycznym określonego w art. 115 §  20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (zgodnie z którym przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu), w przypadku gdy takie materiały bezpośrednio lub pośrednio (np. przez pochwalanie aktów terrorystycznych) popierają popełnianie przestępstwa o charakterze terrorystycznym i tym samym stwarzają niebezpieczeństwo popełnienia jednego lub większej liczby takich przestępstw,
2. nakłaniają osobę lub grupę osób do popełnienia lub przyczynienia się do popełnienia przestępstwa o charakterze terrorystycznym,
3. nakłaniają osobę lub grupę osób do uczestniczenia w działaniach grupy terrorystycznej,
4. udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji lub w zakresie innych szczególnych metod lub technik w celu popełnienia lub przyczynienia się do popełnienia przestępstwa o charakterze terrorystycznym,
5. stwarzają zagrożenie popełnienia przestępstwa o charakterze terrorystycznym.

Z kolei za „dostawcę usług hostingowych” należy uznać dostawcę usług normalnie świadczonych za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług, polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek. Natomiast „dostawcą treści” jest użytkownik, który dostarczył informacje, które są lub były przechowywane i publicznie rozpowszechniane przez dostawcę usług hostingowych.

Równocześnie proponuje się dodanie do ustawy o działaniach antyterrorystycznych rozdziału 5a „Przeciwdziałanie rozpowszechnianiu w internecie treści o charakterze terrorystycznym”, który umożliwi stosowanie unijnych rozwiązań, jednocześnie będąc komplementarnym z rozwiązaniami przyjmowanymi w tym zakresie przez pozostałe państwa członkowskie UE.

Celem dodania **art. 26a** ustawy jest ustanowienie na gruncie ustawowym Szefa ABW jako organu właściwego w rozumieniu rozporządzenia 2021/784. W rezultacie Szef ABW będzie odpowiedzialny m.in. za:

1. wydawanie nakazów zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści terrorystycznych we wszystkich państwach członkowskich, zgodnie z art. 3 rozporządzenia 2021/784,
2. weryfikowanie nakazów usunięcia wydanych przez właściwe organy innych państw członkowskich oraz stwierdzania ewentualnych naruszeń w tym zakresie, zgodnie z art. 4 rozporządzenia 2021/784,
3. przedłużanie okresu zachowania treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony, na skutek wydanego nakazu usunięcia (art. 6 ust. 2 rozporządzenia 2021/784),
4. wydawanie decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym oraz nadzoru nad wdrażaniem przez nich środków szczególnych, na podstawie art. 5 rozporządzenia 2021/784,
5. prowadzenie współpracy, w tym wymiany informacji, z innymi właściwymi organami ustanowionymi przez pozostałe państwa członkowskie, Europolem oraz dostawcami usług hostingowych, zgodnie z art. 14 rozporządzenia 2021/784,
6. nakładanie kar administracyjnych, na podstawie art. 18 rozporządzenia 2021/784,
7. publikację sprawozdania, na podstawie art. 8 rozporządzenia 2021/784,
8. przekazywanie do Komisji Europejskiej rocznej informacji, na podstawie art. 21 rozporządzenia 2021/784.

Nakazy usunięcia Szef ABW będzie mógł wydawać wszystkim dostawcom usług hostingowych obowiązanym do przestrzegania przepisów rozporządzenia 2021/784. Natomiast w pozostałym zakresie działania Szefa ABW wynikające ze stosowania rozporządzenia 2021/784 będą ograniczone wyłącznie do dostawców usług hostingowych, którzy mają główną jednostkę organizacyjną w Polsce lub których przedstawiciel prawny ma miejsce pobytu lub siedzibę w Polsce, i tylko w zakresie, o jakim mowa w rozporządzeniu 2021/784.

Mając na uwadze, że przepisy rozporządzenia stosuje się wprost, swoje zadania Szef ABW będzie realizował na zasadach określonych w art. 13 ust. 2 rozporządzenia 2021/784, a zatem w sposób obiektywny i niedyskryminacyjny, z pełnym poszanowaniem praw podstawowych. W kontekście wykonywania zadań, o których mowa w art. 12 ust. 1, nie będzie mógł też zwracać się o instrukcje do żadnego innego organu ani przyjmować takich instrukcji, co jednak nie wyklucza działań podejmowanych w ramach sprawowania nad nim konstytucyjnego nadzoru. Pozycja prawno-ustrojowa Szefa ABW, wynikająca przede wszystkim z ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu zapewnia stosowanie przepisów unijnych w tym zakresie. Zgodnie z ww. ustawą Szef ABW jest centralnym organem administracji rządowej, podlegającym bezpośrednio Prezesowi Rady Ministrów oraz podlegającym kontroli Sejmu RP. Celem ustawowym samej Agencji jest z kolei ochrona bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.

Zgodnie z projektowanym **art. 26b** Szef ABW wyznacza w ramach podległej mu służby punkt kontaktowy właściwy do rozpatrywania wniosków o wyjaśnienie i informacje zwrotne dotyczące nakazów wydanych przez ABW, który będzie funkcjonował całodobowo 7 dni w tygodniu. Dane dotyczące tego punktu, w tym dane kontaktowe oraz sposób składania ww. wniosków, będą publicznie dostępne za pośrednictwem Biuletynu Informacji Publicznej na stronie podmiotowej ABW, a także przekazane do wiadomości Komisji Europejskiej. W ten sposób zostanie wypełniony obowiązek, który unijny prawodawca nakłada na państwa członkowskie w art. 12 ust. 2 rozporządzenia 2021/784 w zakresie wyznaczenie punktu kontaktowego do spraw nakazów usunięcia wydanych w danym państwie.

W myśl **art. 26c** ustawy nadzór Szefa ABW nad dostawcami usług hostingowych w zakresie wdrażania przez nich środków szczególnych będzie polegał na dokonywaniu przez Szefa ABW kontroli środków szczególnych, które dostawca usług hostingowych zdecydował się zastosować, a także na wydawaniu zaleceń w przypadku stwierdzenia nieprawidłowości w tym zakresie. W celu zapewnienia wykonania tych czynności upoważniony funkcjonariusz ABW będzie miał prawo wstępu na teren kontrolowanych obiektów wykorzystywanych do świadczenia usług hostingowych oraz prawo żądania od dostawcy usług hostingowych wyjaśnień i udostępnienia bądź wglądu w dokumentację techniczną i operacyjną wynikającą ze stosowania środków szczególnych. W myśl projektowanych przepisów dostawca usług hostingowych będzie zobowiązany do terminowego usunięcia stwierdzonych nieprawidłowości. Podkreślenia wymaga, że do kontroli, w zakresie nieuregulowanym niniejszą ustawą, będą miały zastosowanie przepisy ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców , w tym art. 48, art. 49 ust. 1–3 i 6–9, a także art. 51–57.

Ponadto wskazać należy, że o ile decyzje Szefa ABW uznające dostawców usług hostingowych za narażonych na treści o charakterze terrorystycznym będą miały charakter natychmiastowej wykonalności, o tyle nie będzie to miało przełożenia na obowiązek natychmiastowego wdrożenia środków szczególnych przez tych dostawców. Zgodnie bowiem z art. 5 ust. 5 rozporządzenia 2021/784 dostawca usług hostingowych narażony na treści o charakterze terrorystycznym powiadamia właściwy organ (Szefa ABW) o środkach, które podjął lub zamierza podjąć w terminie do 3 miesięcy od otrzymania decyzji w tej sprawie. Z kolei w świetle art. 5 ust. 6 rozporządzenia 2021/784 działania kontrolne, o których mowa powyżej, Szef ABW będzie – co do zasady – podejmował nie wcześniej niż po otrzymaniu od dostawcy usług hostingowych tego powiadomienia, a zatem po upływie okresu do 3 miesięcy od wydania decyzji lub też bezpośrednio na wniosek samego dostawcy usług hostingowych.

Powyższe przepisy mają na celu zapewnienie stosowania art. 12 rozporządzenia 2021/784, które nakłada na państwa członkowskie obowiązek wyznaczenia organu właściwego w zakresie wydawania nakazów usunięcia i ich weryfikowaniu, nadzoru nad dostawcami usług hostingowych w zakresie wdrażania środków szczególnych, a także nakładania kar za naruszenia przedmiotowego rozporządzenia.

W świetle proponowanego brzmienia **art. 26d** ustawy do nakazów usunięcia oraz stwierdzania naruszeń, o których mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/784, zastosowanie będzie miała ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego we wskazanym w tym przepisie zakresie. Częściowe zastosowanie uregulowań Kodeksu postępowania administracyjnego w tym przypadku jest niezbędne. Stanowi o tym fakt, że tryb postępowania opisany w rozporządzeniu 2021/784 odnośnie do wydawania nakazów usunięcia ma zapewnić na poziomie unijnym (a zatem w wymiarze transgranicznym) spójny i efektywny mechanizm usuwania lub blokowania w sieci wszelkich treści o charakterze terrorystycznym. Skuteczność tego mechanizmu jest natomiast mierzona szybkością reakcji i wykonania stosownych czynności. W rezultacie przyjęty w unijnym akcie sposób postępowania zarówno w odniesieniu do wydawania nakazów usunięcia, jak i stwierdzenia naruszeń, o których mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/784, znacząco odbiega od niektórych rozwiązań przyjętych na gruncie krajowych przepisów prawa administracyjnego. Ponadto większość elementów w rozumieniu postępowania administracyjnego zostało wprost określonych w samym rozporządzeniu, np. elementy decyzji, moment i skutek jej doręczenia, a zatem w takim przypadku jest niezbędne wyłączenie uregulowań krajowych.

Wymieniony w projektowanym art. 26d ust. 1 katalog przepisów Kodeksu postępowania administracyjnego jest po części wzorowany na funkcjonujących już w analogicznych przypadkach przepisach (np. w art. 4 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego), a po części stanowi niezbędne uzupełnienie i dostosowanie mechanizmu postępowania wynikającego wprost z przepisów rozporządzenia 2012/784. W rezultacie wskazane w niniejszym przepisie art. 50 oraz art. 54–56 k.p.a., dotyczące procedury wezwania, jak również art. 63–65 k.p.a., określające procedurę wnoszenia podania (żądania, wyjaśnienia, odwołania, zażalenia), będą mogły mieć *de facto* zastosowanie wyłącznie w odniesieniu do postępowań w sprawach stwierdzania naruszeń, o których mowa w art. 4 ust. 3 i 4. rozporządzenia 2021/784. Analogicznie do przypadku nakazów usunięcia oraz stwierdzania naruszeń, wskazanie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, zgodnie z art. 5 rozporządzenia 2021/784, będzie następowało w formie decyzji. Do tych decyzji również będzie miał zastosowanie Kodeks postępowania administracyjnego tylko w zakresie wskazanym niniejszym projektem. Jednocześnie przewiduje się, że we wszystkich tych przypadkach postępowania będą jednoinstancyjne, a wydane decyzje będą podlegały natychmiastowej wykonalności. Tryb jednoinstancyjny jest w tym przypadku niezbędny w celu zapewnienia sprawności i efektywności prowadzenia takich postępowań. Takie rozwiązanie pozostaje zgodne z Konstytucją RP, która w art. 78 przewiduje możliwość ustawowego odstępstwa od zaskarżenia orzeczeń i decyzji wydanych w pierwszej instancji. Zgodnie z ustawą zasadniczą tego rodzaju ograniczenia mogą być ustanawiane wyłącznie ustawą i gdy jest to konieczne m.in. z uwagi na kwestie bezpieczeństwa i porządku publicznego. Kontekst i *ratio legis* projektu wpisują się zatem w te przesłanki. Natomiast mając na uwadze, że dostawcy usług hostingowych i dostawcy treści będzie każdorazowo przysługiwało prawo wniesienia skargi do sądu, istota wolności i praw pozostanie w tym przypadku zachowana.

Prawo do zaskarżenia będzie przysługiwało dostawcom usług hostingowych również w odniesieniu do decyzji Szefa ABW wydanych na podstawie art. 5 ust. 6 lub 7 rozporządzenia 2021/784 . Wskazać należy, że projektowany art. 26d w tym zakresie stanowi wypełnienie art. 9 rozporządzenia 2021/784, który m.in. przewiduje prawo do zaskarżania wydanych nakazów usunięcia oraz pozostałych decyzji wydanych przez organ właściwy.

W przypadku gdy strona nie zawnioskuje o przeprowadzenie rozprawy, sąd – jeżeli uzna, że wszystkie okoliczności sprawy zostały dostatecznie wyjaśnione – będzie mógł zdecydować o jej rozpoznaniu w trybie uproszczonym. Nie wyklucza to jednak sytuacji, że rozpoznając sprawę w trybie uproszczonym, sąd ostatecznie zdecyduje o jej rozpoznaniu na rozprawie. Tryb uproszczony będzie mógł mieć zatem zastosowanie jedynie fakultatywnie po spełnieniu łącznie obu przesłanek i ma – co do zasady – zapewnić, że rozpatrywanie środków prawnych od nakazów usunięcia oraz od decyzji o wskazaniu dostawcy usług hostingowych narażonych na treści o charakterze terrorystycznym będzie realizowane w sposób sprawny i efektywny, ale z zachowaniem wszelkich gwarancji prawa do sądu.

W postępowaniach, o których mowa powyżej, właściwy pozostaje sąd administracyjny, co wynika z faktu, że postępowania te będą dotyczyły wyłącznie kwestii prawno‑administracyjnych. Należy zauważyć, że określone rozporządzeniem 2021/784 sankcje odnoszą się do sytuacji niespełnienia określonych obowiązków o charakterze administracyjnym przez dostawcę usług hostingowych, nie zaś dopuszczenia się przez nich czynów karalnych na gruncie przepisów prawa karnego materialnego. Samo usuwanie treści nie jest środkiem sankcyjnym, lecz środkiem ograniczającym. W związku z tym projektodawca przewiduje, że w tym zakresie jedynie sądy administracyjne będą kompetentnymi jednostkami sądownictwa do rozpatrywania skarg na decyzje Szefa ABW.

Mając na uwadze potrzebę zapewnienia wykonania art. 21 ust. 1 rozporządzenia 2021/784, który zobowiązuje państwa członkowskie do gromadzenia i przekazywania do Komisji Europejskiej informacji m.in. w zakresie podjętych środków szczególnych, liczby wszczętych procedur rozpatrywania skarg oraz innych działań podjętych przez dostawcę usług hostingowych w ramach ustanowionego mechanizmu skargowego, dostawcy usług hostingowych – na podstawie **art. 26e** ustawy – będą zobowiązani do cyklicznego przekazywania do Szefa ABW informacji, o których mowa w art. 21 ust. 1 lit. b i d rozporządzenia 2021/784. Dane te następnie będą zbiorczo przesyłane do wiadomości Komisji Europejskiej.

Projektowane art. 26f–26h stanowią natomiast konsekwencję przepisów unijnych, które w art. 18 rozporządzenia 2021/784 zobowiązują państwa członkowskie do ustanowienia środków karnych mających zastosowanie w przypadku naruszeń tego rozporządzenia. Należy zauważyć, że przepisy unijne szczegółowo wskazują zarówno rodzaj naruszeń podlegających karze (art. 18 ust. 1), jak i okoliczności, które należy uwzględnić przy określeniu wysokości tej kary (art. 18 ust. 2 i 3).

W związku z powyższym proponuje się w **art. 26f ust. 1** bezpośrednie odesłanie do określonego w art. 18 ust. 1 rozporządzenia 2021/784 katalogu przypadków naruszeń, które będą sankcjonowane odpowiednimi karami. Z kolei w projektowanym art. 26f ust. 2 proponuje się przyznanie Szefowi ABW uprawnienia do nakładania na dostawców usług hostingowych, w drodze decyzji administracyjnej, kar pieniężnych za popełnienie tych naruszeń. Przy nakładaniu kar będą brane pod uwagę warunki i okoliczności określone w art. 18 rozporządzenia 2021/784 w wysokości do 4% całkowitych obrotów uzyskanych przez tego dostawcę w poprzednim roku obrotowym. W takiej wysokości kara będzie mogła zostać nałożona jednak wyłącznie w przypadku, gdy dostawca systematycznie lub uporczywie nie będzie wypełniał obowiązków w zakresie usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich.

Zgodnie bowiem z unijnymi regulacjami wysokość kar pieniężnych powinna być skuteczna, proporcjonalna i odstraszająca w zależności od zaistniałych okoliczności analizowanych w każdym przypadku indywidualnie. Mając na uwadze powyższe, organ właściwy, ustalając wysokość kary, będzie musiał wziąć pod uwagę szereg istotnych okoliczności, w tym te określone w art. 18 ust. 2 rozporządzenia 2021/784, tj.:

1. charakter, wagę i czas trwania naruszenia,
2. umyślny lub wynikający z zaniedbania charakter naruszenia,
3. wcześniejsze naruszenia popełnione przez dostawcę usług hostingowych,
4. kondycję finansową dostawcy usług hostingowych,
5. poziom współpracy dostawcy usług hostingowych z właściwymi organami,
6. charakter i rozmiary dostawców usług hostingowych, w szczególności, czy jest on mikro-, małym lub średnim przedsiębiorstwem,
7. stopień winy dostawcy usług hostingowych, z uwzględnieniem podjętych przez niego środków technicznych i organizacyjnych w celu spełnienia wymogów niniejszego rozporządzenia.

Jednocześnie proponuje się, aby należności z tytułu kar pieniężnych stanowiły dochód budżetu państwa, a postępowania w tych sprawach były jednoinstancyjne.

Uzupełnieniem powyższej regulacji będą przepisy prawa krajowego, w tym projektowany **art. 26g** ustawy, w którym proponuje się, aby przy ustalaniu wysokości kary Szef ABW miał możliwość zwrócenia się do dostawcy usług hostingowych, wobec którego prowadzone jest postępowanie w sprawie nałożenia kary pieniężnej, o dostarczenie odpowiednich informacji. Dostawca będzie miał ustawowo 30 dni na dostarczenie stosownej dokumentacji. W przypadku gdy w tym terminie nie poda żądanych informacji, Szef ABW ustali podstawę wymiaru kary pieniężnej w sposób szacunkowy, biorąc pod uwagę ogólnie dostępne dane finansowe tego przedsiębiorcy.

Wskazać też należy, że projekt w zakresie nakładania kar nie przewiduje wyłączenia przepisów powszechnie obowiązujących, czyli w tym przypadku Kodeksu postępowania administracyjnego, a zatem, wymierzając karę, organ będzie miał możliwość skorzystania z narzędzi łagodzących jej ostateczny wymiar, tj. np. z instytucji odroczenia albo rozłożenia na raty stosownie do popełnionego naruszenia oraz innych możliwości określonych przepisami (art. 189k k.p.a.). Dodatkowo podkreślenia wymaga, że chociaż projektodawca założył ustanowienie wyłącznie systemu kar pieniężnych, to jednak zasada proporcjonalności zostanie zachowana również dzięki możliwości zastosowania przez organ przepisów pozwalających na odstąpienie od kary pieniężnej na rzecz lżejszej formy ukarania, np. pouczenia, przy założeniu zaistnienia ku temu określonych prawem przesłanek – *vide* art. 189f k.p.a.

Natomiast w **art. 26h** przewiduje się uregulowanie terminu płatności administracyjnych kar pieniężnych.

Dodanie rozdziału 5a w ustawie o działaniach antyterrorystycznych wymaga modyfikacji dotychczasowych przepisów odnoszących się do kwestii zarządzania blokady dostępności w internecie. W związku z tym w art. 2 niniejszego projektu proponuje się wprowadzenie stosownych zmian do obowiązującego **art. 32c** ustawy  Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, który przewiduje, że – co do zasady – w celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym lub przestępstwa szpiegostwa oraz ścigania ich sprawców, sąd na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, 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 uprawdopodabniającym popełnienie przestępstwa szpiegostwa lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa. Jednocześnie wskazać należy, że przepis ten stanowi wdrożenie art. 21 dyrektywy 2017/541 z dnia 15 marca 2017 r., który nakłada na państwa członkowskie obowiązek zapewnienia natychmiastowego usuwania treści internetowych publicznie nawołujących do popełnienia przestępstwa terrorystycznego, nie wskazując przy tym podmiotu zobowiązanego do usuwania takich treści. Z kolei rozporządzenie 2021/784 nakłada zobowiązania do usuwania treści o charakterze terrorystycznym wyłącznie na dostawców usług hostingowych, nie nakładając takich obowiązków na inne podmioty świadczące usługi drogą elektroniczną, w tym np. usługi tzw. cachingu, które należy rozumieć jako usługi polegające na automatycznym i krótkotrwałym przechowywaniu na serwerze pośredniczącym cudzych danych przez stworzenie ich kopii w celu ich szybszego udostępnienia użytkownikowi końcowemu. W tym kontekście podkreślenia wymaga również to, że przepisy ww. dyrektywy nie zostały uchylone rozporządzeniem 2021/784, co oznacza, że oba akty są względem siebie komplementarne i powinny być stosowane równolegle.

Mając powyższe na uwadze, niniejszy projekt zakłada utrzymanie w mocy art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu z jednoczesną jego modyfikacją, która zapewni, że przepis ten będzie miał zastosowanie w przypadkach publikowania lub prób publikowania w internecie treści o charakterze terrorystycznym przez podmioty niebędące dostawcami usług hostingowych w rozumieniu rozporządzenia 2021/784.

Jednocześnie, mając na uwadze zarzuty Komisji Europejskiej odnośnie do nieprawidłowej transpozycji art. 21 ust. 1 dyrektywy 2017/541, proponuje się uzupełnienie art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu o element usuwania treści o charakterze terrorystycznym. W art. 21 ust. 1 dyrektywa 2017/541 zobowiązuje państwa członkowskie do wprowadzenia niezbędnych środków w celu zapewnienia natychmiastowego usuwania treści internetowych o charakterze terrorystycznym, a przynajmniej tych, które znajdują się na serwerach na ich terytorium. Z kolei zgodnie z art. 21 ust. 2 tej dyrektywy państwa członkowskie mogą wprowadzić środki w celu zablokowania użytkownikom korzystającym z internetu na ich terytorium dostępu do takich treści, jednakże tylko w przypadku, gdy usunięcie takich treści u źródła nie jest możliwe. W ocenie Komisji Europejskiej transpozycja art. 21 ust.1 dyrektywy przez Polskę jest nieprawidłowa. W swoim stanowisku Komisja Europejska stwierdza: „Polskie prawo nie przewiduje środków zapewniających natychmiastowe usuwanie takich treści internetowych, w szczególności gdy takie treści znajdują się na serwerach na terytorium Polski. Chociaż może się to różnić w niektórych indywidualnych przypadkach, nie ma powodu, aby sądzić, że usunięcie treści u źródła byłoby zasadniczo niewykonalne. Art. 21 ust. 2 nie może być rozumiany jako powód, dla którego państwo członkowskie nie dokonało transpozycji art. 21 ust. 1. Zgodnie z dyrektywą państwa członkowskie są bowiem zobowiązane do transpozycji obu przepisów, tak aby możliwe było usunięcie treści zgodnie z art. 21 ust. 1 jako zasada ogólna oraz zablokowanie dostępu zgodnie z art. 21 ust. 2, jeżeli w indywidualnych przypadkach usunięcie nie jest wykonalne.”[[6]](#footnote-6)).

W rezultacie proponuje się w art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu ustanowienie podstawy prawnej do zarządzania wobec usługodawców świadczących usługi drogą elektroniczną usunięcia lub zablokowania dostępności określonych danych lub usług teleinformatycznych, a wobec przedsiębiorców telekomunikacyjnych – zablokowania dostępności takich danych lub usług. Wyłączenie przedsiębiorców telekomunikacyjnych z obowiązku usuwania danych lub usług telekomunikacyjnych wynika z braku ich uprawnienia do podejmowania tego rodzaju czynności.

Jednocześnie wyjaśnić należy, że rozszerzenie zakresu przedmiotowego art. 32c ust. 1 o mechanizm usunięcia określonych danych teleinformatycznych nie będzie miało istotnego przełożenia na zwiększenie zadań organów, o których mowa w tym przepisie. Obowiązek prowadzenia rejestru stosownych postanowień, pisemnych zgód, zarządzeń i wniosków wynika już z obowiązujących przepisów wydanych na podstawie upoważnienia ustawowego z art. 32c ust. 14 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Projektowane zmiany spowodują dodanie do tego katalogu jedynie dokumentacji, która będzie wytworzona na potrzeby zarządzenia usunięcia określonych danych informatycznych. Mając zaś na uwadze, że w świetle obowiązujących przepisów większość dokumentów jest wytwarzana przez przedstawicieli organów ścigania, proponowane zmiany nie wpłyną znacząco również na kognicję i obowiązki sądów.

W celu uporządkowania stosowania przepisów prawa unijnego w zakresie usuwania i blokowania internetowych treści o charakterze terrorystycznym, w myśl dyrektywy 2017/541 oraz rozporządzenia 2021/784 proponuje się wskazanie przepisu wyłączającego stosowanie mechanizmów usuwania lub blokowania, o których mowa w art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, w odniesieniu do dostawców usług hostingowych oraz treści o charakterze terrorystycznym, o których mowa w rozporządzeniu 2021/784.

Mając na uwadze, że niniejszy projekt przewiduje modyfikację upoważnienia ustawowego do wydania rozporządzenia przez Prezesa Rady Ministrów dotychczas obowiązującego na podstawie art. 32c ust. 14, w art. 3 niniejszego projektu proponuje się wprowadzenie przepisu przejściowego, utrzymującego w mocy dotychczasowe rozwiązania do czasu przyjęcia nowego rozporządzenia.

Ponadto przewiduje się wprowadzenie przepisu przejściowego, który zapewni, że do blokad dostępności, już zarządzonych i niezakończonych przed dniem wejścia w życie projektowanej ustawy, stosuje się przepisy dotychczasowe.

Projekt uwzględnia wyrażone w art. 67 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorcówzasady proporcjonalności i adekwatności projektowanych rozwiązań, a zapewniając stosowanie prawa Unii Europejskiej, któremu służy niniejsza regulacja, dokonano nałożenia jedynie takich obowiązków administracyjnych, jakie wynikają bezpośrednio z przepisów rozporządzenia 2021/784. Ponadto, zgodnie ze wskazanym rozporządzeniem, umożliwiono realizację obowiązków informacyjnych w postaci elektronicznej.

Zgodnie z art. 24 rozporządzenia 2021/784 jest ono stosowane od dnia 7 czerwca 2022 r. Do tego dnia państwa członkowskie powinny powiadomić Komisję Europejską o właściwych wyznaczonych organach, a Komisja Europejska ma stworzyć internetowy wykaz tych organów oraz wyznaczonych w nich punktach kontaktowych.

Mając na względzie, że rozporządzenie 2021/784 weszło w życie z dniem 7 czerwca 2021 r., niezbędne jest, aby projektowane zmiany zostały wprowadzone do polskiego porządku prawnego jak najszybciej. Wobec powyższego przewiduje się, że projektowana ustawa wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

W dniu 7 lutego 2024 r. Komisja Europejska skierowała do Rzeczypospolitej Polskiej, na mocy art. 258 Traktatu o funkcjonowaniu Unii Europejskiej, uzasadnioną opinię w związku z niedopełnieniem niektórych obowiązków wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym. W opinii tej Komisja Europejska zobowiązała Polskę do przedsięwzięcia wymaganych środków w terminie dwóch miesięcy od wpływu opinii. W efekcie Polska musi zapewnić pilną realizację ciążących na niej obowiązków.

Projekt ustawy nie zawiera przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.) i w związku z tym nie podlega procedurze notyfikacji.

Projekt ustawy jest zgodny z przepisami prawa Unii Europejskiej i służy ich stosowaniu.

Projekt ustawy nie podlega przedstawieniu właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt ustawy stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348 oraz z 2024 r. poz. 757) został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny. W trybie ww. ustawy uwag do projektu nie zgłoszono.

Projekt ustawy nie podlegał dokonaniu oceny OSR przez koordynatora OSR w trybie § 32 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów.

1. ) Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania rozporządzenia (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym z 14.02.2024 r. (COM(2024) 64 final), str. 1. [↑](#footnote-ref-1)
2. ) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/WSiSW (Dz. Urz. UE L 88 z 31.03.2017, str. 6). [↑](#footnote-ref-2)
3. ) https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points\_en (dostęp: 07.03.2024 r.) [↑](#footnote-ref-3)
4. ) „Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania rozporządzenia (UE) 2021/784 (…) str. 6. [↑](#footnote-ref-4)
5. ) Str. 14 Sprawozdania, o którym mowa w odnośniku nr 4. [↑](#footnote-ref-5)
6. ) Stanowisko Komisji Europejskiej z 9 czerwca 2021 r. (sygn. INFR(2021)2046, C(2021)3630 final, str. 7. [↑](#footnote-ref-6)