Terroryzm – studia, analizy, prewencja, 2025, nr 7: 35–92

https://doi.org/10.4467/27204383TER.25.026.21803

Artykuł

Komentarz do zmiany ustawy o działaniach antyterrorystycznych w związku z przeciwdziałaniem rozpowszechnianiu w internecie treści o charakterze terrorystycznym

Commentary on the amendment of the Act on anti-terrorist activities in relation to countering the dissemination of terrorist content on the internet

MARIUSZ CICHOMSKI

https://orcid.org/0000-0003-3707-7856

Ministerstwo Spraw Wewnętrznych i Administracji

Abstrakt

Artykuł stanowi komentarz do *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* w zakresie przepisów wprowadzonych do tej regulacji *Ustawą z dnia 18 października 2024 r. o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*. Celem wprowadzonych przepisów jest zapewnienie stosowania w polskim porządku prawnym *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*. Autor przywołał poprzednie nowelizacje ustawy o działaniach antyterrorystycznych oraz omówił podstawowe rozwiązania zawarte w rozporządzeniu 2021/784 dotyczące dostawców usług hostingowych – nakazy usunięcia treści o charakterze terrorystycznym oraz środki szczególne, czyli wydawanie decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym.

Słowa kluczowe

terroryzm, blokowanie treści w internecie, ustawa o działaniach antyterrorystycznych, treści o charakterze terrorystycznym, dostawca usług hostingowych, dostawca treści

Abstract

The article is a commentary on the *Act of 10 June 2016 on anti-terrorist activities* in terms of the provisions introduced to this regulation by the *Act of 18 October 2024 amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency*. The purpose of the introduced provisions is to ensure the application in the Polish legal order of the *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online*. The author recalled previous amendments to the Act on anti-terrorist activities and discussed the basic solutions contained in Regulation 2021/784 concerning hosting providers – orders to remove terrorist content and special measures, i.e. issuing decisions on hosting providers exposed to terrorist content.

Keywords

terrorism, internet content blocking, the act on anti-terrorist activities, terrorist content, hosting provider, content provider

Wprowadzenie. Dotychczasowe nowelizacje ustawy o działaniach antyterrorystycznych

Ustawą z dnia 18 października 2024 r. o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu zapewniono stosowanie w polskim porządku prawnym *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym* (dalej: rozporządzenie 2021/784), co zostało zrealizowane przez nowelizację *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (dalej: ustawa o działaniach AT). Regulacją z 18 października 2024 r. dokonano również, przez nowelizację *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (dalej: ustawa

o ABW oraz AW), uzupełniającej implementacji *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującej decyzję ramową Rady 2002/475/WSiSW oraz zmieniającej decyzję Rady 2005/671/WSiSW* (dalej: dyrektywa 2017/541).

Była to pierwsza tak istotna zmiana ustawy o działaniach AT od momentu jej uchwalenia w 2016 r., czyli po blisko dziewięciu latach obowiązywania. Zmiana ta polegała zarówno na rozszerzeniu zakresu przedmiotowego normowania regulacji, jak i objęciu nią nowych kategorii adresatów. Poprzednie nowelizacje, choć ich liczba (12) może wydawać się stosunkowo wysoka, miały charakter dostosowujący, korygujący czy usprawniający w odniesieniu do wdrożonych wcześniej mechanizmów i nie wprowadzały nowych instytucji prawnych w istotny sposób zmieniających zakres stosowania tej ustawy.

W pięciu przypadkach zmiany dotyczyły uwzględnienia podmiotu, który powstał wskutek przekształcenia innego podmiotu po wejściu w życie pierwotnej wersji ustawy o działaniach AT. Były to: powstanie Krajowej Administracji Skarbowej w miejsce rozproszonych struktur resortu finansów, zwłaszcza Służby Celnej, kontroli skarbowej, wywiadu skarbowego i administracji podatkowej[1], przekształcenie Biura Ochrony Rządu w Służbę Ochrony Państwa[2], zmiana statusu Straży Marszałkowskiej na państwową służbę mundurową oraz korekta jej zadań[3], uwzględnienie, pominiętego wcześniej wskutek zmieniającego się statusu, Generalnego Inspektora Informacji Finansowej[4] czy ustawowe przypisanie Prokuratorowi Krajowemu zadań przynależnych dotychczas Prokuratorowi Generalnemu[5].

Kolejna grupa nowelizacji to trzy przypadki zmian związane z uspójnieniem z innymi powstającymi lub zmieniającymi się ustawami w celu zachowania legislacyjnej zgodności odesłań bądź poprawności terminologicznej. W ten sposób należy odczytywać zmiany wprowadzone *Ustawą z dnia 6 marca 2018 r. – Prawo przedsiębiorców*, *Ustawą z dnia 21 stycznia*

[1] *Ustawa z dnia 16 listopada 2016 r. – Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej*. W artykule przedstawiono stan prawny na 23 II 2025 r.

[2] *Ustawa o Służbie Ochrony Państwa z dnia 8 grudnia 2017 r.*

[3] *Ustawa z dnia 26 stycznia 2018 r. – Przepisy wprowadzające ustawę o Straży Marszałkowskiej*.

[4] *Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw*.

[5] *Ustawa z dnia 7 lipca 2023 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Prawo o ustroju sądów powszechnych, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw*.

2021 r. o służbie zagranicznej oraz *Ustawą z dnia 11 marca 2022 r. o obronie Ojczyzny*.

Ostatnia grupa zmian to cztery nowelizacje mające wprawdzie znaczenie merytoryczne, lecz ich charakter był wycinkowy i miały one stanowić usprawnienie lub skorygowanie dotychczasowych przepisów z perspektywy praktyki stosowania prawa. *Ustawą z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa* doprecyzowano art. 13 ustawy o działaniach AT, normujący zagadnienia związane z zakładaniem tymczasowych instalacji radiokomunikacyjnych oraz budową, przebudową lub instalowaniem infrastruktury przewodowej i innych urządzeń lub infrastruktury w zakresie niezbędnym do uruchomienia i prawidłowego użytkowania tych instalacji. Ponadto do ustawy o działaniach AT dodano art. 13a, zgodnie z którym Prezes Rady Ministrów, z uwagi na możliwość wystąpienia zdarzenia o charakterze terrorystycznym albo zagrożenia bezpieczeństwa i porządku publicznego, może, w drodze zarządzenia, ograniczyć publiczny dostęp do wykazów, rejestrów, baz danych i systemów teleinformatycznych zawierających dane lokalizacyjne infrastruktury technicznej.

Ustawą z dnia 7 lipca 2023 r. o zmianie ustawy o ochronie żeglugi i portów morskich oraz niektórych innych ustaw dokonano korekty dotyczącej zakresu art. 24 ustawy o działaniach AT przez uwzględnienie polskiej wyłącznej strefy ekonomicznej jako obszaru, w którym mogą być prowadzone działania antyterrorystyczne. Zgodnie z nowym brzmieniem przepisu działania antyterrorystyczne na zasadach określonych w tej ustawie mogą być prowadzone poza granicami RP, na akwenach w polskiej strefie odpowiedzialności SAR (ang. *search and rescue*), zgodnie z *Międzynarodową Konwencją o poszukiwaniu i ratownictwie morskim, sporządzoną w Hamburgu dnia 27 kwietnia 1979 r.,* i w polskiej wyłącznej strefie ekonomicznej. Analogicznie służby ratownicze mogą prowadzić działania zmierzające do usunięcia skutków zdarzenia o charakterze terrorystycznym i w tym zakresie współdziałają ze sobą oraz ze służbami prowadzącymi działania antyterrorystyczne na ww. obszarach. W pierwotnej wersji przepis ten ograniczał obszar działania do strefy odpowiedzialności SAR.

Kolejna zmiana została wprowadzona *Ustawą z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw* i dotyczyła dwóch najbardziej kontrowersyjnych z perspektywy konstytucyjnej, w opinii autora, przepisów ustawy o działaniach AT. Pierwsza zmiana modyfikowała art. 9 ustawy, stanowiący podstawę do prowadzenia przez Szefa ABW

kontroli operacyjnej w odniesieniu do cudzoziemców w celu rozpoznawania, zwalczania i wykrywania przestępstw o charakterze terrorystycznym i zapobiegania im oraz ścigania ich sprawców. Przepis ten został rozszerzony o dodatkową przesłankę, tj. przestępstwo szpiegostwa[6]. Druga zmiana dotyczyła art. 26 ust. 2 – wydłużono do 30 dni maksymalny termin tymczasowego aresztowania zastosowanego na podstawie tej ustawy. Wprowadzone zmiany zakładały zwiększenie możliwości praktycznego zastosowania ww. przepisów. Ich celem nie było jednak dokonanie zmian mogących minimalizować wątpliwości natury konstytucyjnej[7].

Nieco większy zakres zmian został wprowadzony do ustawy o działaniach AT *Ustawą z dnia 26 lipca 2024 r. o zmianie niektórych ustaw w celu usprawnienia działań Sił Zbrojnych Rzeczypospolitej Polskiej, Policji oraz Straży Granicznej na wypadek zagrożenia bezpieczeństwa państwa*. Zmiany te nie tworzyły jednak nowych instytucji prawnych. Ich celem było natomiast podniesienie funkcjonalności wcześniejszych rozwiązań przez wprowadzenie możliwości przekazania opinii co do zasadności wprowadzenia, zniesienia lub zmiany stopnia alarmowego także ustnie, telefonicznie, za pomocą środków komunikacji elektronicznej (art. 16 ustawy o działaniach AT)[8]. Analogiczne rozwiązanie przyjęto także do przekazywania wniosku o uruchomienie pomocy dla Policji ze strony Sił Zbrojnych RP (art. 22 ustawy o działaniach AT). Ujednolicono także zapisy z *Ustawą z dnia 6 kwietnia 1990 r. o Policji* przez wskazanie, że żołnierzom oddziałów i pododdziałów Wojsk Specjalnych użytych do pomocy oddziałom i pododdziałom Policji

[6] W tym kontekście warto przywołać przede wszystkim wyrok Europejskiego Trybunału Praw Człowieka (ETPCz) w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce, w którym ETPCz uznał, że doszło do naruszenia art. 8 *Konwencji o ochronie praw człowieka i podstawowych wolności* w związku ze sposobem ukształtowania systemu kontroli operacyjnej w Polsce. ETPCz zwrócił uwagę, że w odniesieniu do kontroli operacyjnej prowadzonej na podstawie ustawy o działaniach AT ani wprowadzenie niejawnego nadzoru, ani jego stosowanie w początkowym trzymiesięcznym okresie nie podlega żadnej kontroli ze strony niezależnego organu zewnętrznego w stosunku do funkcjonariuszy ABW prowadzących ten nadzór. Zob. Wyrok Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce, https://arch-bip.ms.gov.pl/pl/prawa-czlowieka/europejski-trybunal-praw-czlowieka/orzecznictwo-europejskiego-trybunalu--praw-czlowieka/listByYear,2.html?ComplainantYear=2024 [dostęp: 18 V 2025].

[7] Zob. szerzej: M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz*, Warszawa 2018, s. 36, 76–116, 213–214, 224–229.

[8] Kwestia ta jako postulat de lege ferenda została wskazana w: M. Cichomski, I. Idzikowska-Ślęzak, *Stopnie alarmowe – praktyczny i prawny wymiar ich stosowania*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 65. https://doi.org/10.4467/27204383TER.22.018.16338.

przysługują, w zakresie niezbędnym do wykonywania ich zadań, uprawnienia funkcjonariuszy Policji, a korzystanie z tych uprawnień następuje na zasadach i w trybie określonych dla funkcjonariuszy Policji (również art. 22 ustawy o działaniach AT).

Konieczność zapewnienia polskich ram stosowania rozporządzenia 2021/784

Na początek warto zadać pytanie, czy zapewnienie stosowania rozporządzenia 2021/784 wymagało wprowadzenia zmian na poziomie ustawowym, a jeśli tak, to czy mogło się ono odbyć na podstawie innych regulacji niż ustawa o działaniach AT. Ograniczone ramy opracowania nie pozwalają na całościowy komentarz do poszczególnych przepisów rozporządzenia 2021/784, dlatego też, na potrzeby tego artykułu, dokonano jedynie syntetycznego omówienia głównych instrumentów prawnych wprowadzonych przez to rozporządzenie w celu zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym. W części będącej komentarzem do poszczególnych przepisów zostały omówione podstawowe regulacje rozporządzenia 2021/784 w odniesieniu do polskich rozwiązań, a także kwestia wyboru na gruncie krajowym organu właściwego do wykonania zobowiązań wynikających z rozporządzenia 2021/784, z uwzględnieniem rozwiązań instytucjonalnych przyjętych w innych państwach UE. Ponadto opisano procedury wydawania i zaskarżania nakazów wynikających ze wskazanego rozporządzenia.

Jak wspomniano we wprowadzeniu, ustawą o zmianie ustawy o działaniach AT i ustawy o ABW oraz AW uzupełniono również wcześniejszą implementację dyrektywy 2017/541. Należy podkreślić, że o ile zapewnieniu stosowania rozporządzenia 2021/784 służyła zmiana ustawy o działaniach AT, o tyle transpozycję dyrektywy 2017/541 zapewniła zmiana ustawy o ABW oraz AW. Połączenie w ramach jednej ingerencji ustawodawczej wykonania obu tych aktów prawa UE należy ocenić jako optymalne rozwiązanie, chociaż obie regulacje, mimo zbieżności obszarów, których dotyczą, związanej z usuwaniem i blokowaniem treści w internecie, mają inny zakres stosowania i nie nakładają się na siebie.

Rozporządzenie 2021/784 weszło w życie 7 czerwca 2021 r., a państwa członkowskie musiały w ciągu jednego roku dostosować do niego swoje regulacje. Jest ono pierwszym kompleksowym aktem prawnym bezpośredniego

stosowania na poziomie UE normującym zagadnienia związane z przeciwdziałaniem rozpowszechnianiu w internecie treści o charakterze terrorystycznym. Poprzedziły go jednak inne inicjatywy. Na przykład w 2015 r. wprowadzono ramy dobrowolnej współpracy między państwami członkowskimi a dostawcami usług hostingowych. Na posiedzeniu w dniach 22–23 czerwca 2017 r. Rada Europejska w odpowiedzi na ataki o charakterze terrorystycznym, do których doszło w krajach UE, oraz związaną z nimi propagandę rozpowszechnianą w internecie stwierdziła, że:

> „oczekuje, że branża [...] opracuje nowe technologie i narzędzia usprawniające automatyczne wykrywanie treści podżegających do aktów terrorystycznych i usuwanie tych treści". W rezolucji z dnia 15 czerwca 2017 r. Parlament Europejski wezwał te platformy internetowe „do wzmocnienia środków zwalczania nielegalnych i szkodliwych treści". Wezwanie przedsiębiorstw do przyjęcia bardziej proaktywnego podejścia, jeśli chodzi o ochronę ich użytkowników przed treściami o charakterze terrorystycznym, zostało powtórzone przez ministrów państw członkowskich w ramach Forum UE ds. Internetu[9].

Dnia 28 września 2017 r. Komisja Europejska (KE) przyjęła komunikat zawierający wytyczne dotyczące obowiązków dostawców usług online w odniesieniu do nielegalnych treści w internecie[10]. Następnie wydała *Zalecenie Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie*, które w rozdziale 3 określiło szczegółowe zalecenia dotyczące treści o charakterze terrorystycznym. Zalecenie to było następstwem wezwania Parlamentu Europejskiego do wzmocnienia środków przeciwdziałania nielegalnym i szkodliwym treściom w internecie, zgodnie z ramami horyzontalnymi ustanowionymi w *Dyrektywie 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego*, a także zgodnie z odpowiedzią na wezwania

[9] Motyw 5 *Zalecenia Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie*.

[10] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Zwalczanie nielegalnych treści w internecie. W kierunku większej odpowiedzialności platform internetowych*, Bruksela, 28 IX 2017 r., COM (2017) 555 final.

Rady Europejskiej do usprawnienia wykrywania i usuwania treści w internecie, które podżegają do aktów terrorystycznych.

Kolejnym krokiem stało się przyjęcie rozporządzenia 2021/784. Za KE warto zauważyć, że: *Ramy regulacyjne dotyczące zwalczania nielegalnych treści w internecie zostały dodatkowo wzmocnione wraz z wejściem w życie 16 listopada 2022 r. aktu o usługach cyfrowych. Akt o usługach cyfrowych reguluje obowiązki dostawców usług cyfrowych, którzy pełnią rolę pośredników w łączeniu konsumentów z treściami, usługami i towarami, tym samym zapewniając lepszą ochronę użytkowników w internecie i przyczyniając się do bezpieczniejszego środowiska internetowego*[11]. Na podstawie tego aktu KE zyskała uprawnienia nadzorcze i wykonawcze do podejmowania działań wobec dużych platform internetowych i wyszukiwarek internetowych. Może ona m.in. kierować wnioski o udzielenie informacji i prowadzić postępowania w sprawie działań przedsiębiorstw w zakresie moderowania treści, wraz z możliwością nakładania grzywien.

Podstawowym motywem wydania rozporządzenia 2021/784 było zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego w otwartym i demokratycznym społeczeństwie przez przeciwdziałanie wykorzystywaniu usług hostingowych do celów terrorystycznych oraz przyczynienie się do poprawy bezpieczeństwa publicznego w całej Unii[12]. Założeniem UE była również poprawa funkcjonowania jednolitego rynku cyfrowego przez zwiększenie pewności prawa dla dostawców usług hostingowych i zaufania użytkowników do środowiska internetowego, a także wzmocnienie gwarancji dotyczących wolności wypowiedzi, w tym wolności otrzymywania i przekazywania informacji i idei w otwartym i demokratycznym społeczeństwie oraz wolności i pluralizmu mediów. Unijny prawodawca dostrzegł, że dostawcy usług hostingowych działający w internecie odgrywają kluczową rolę w gospodarce cyfrowej przez łączenie przedsiębiorstw i obywateli, a także ułatwianie publicznej debaty oraz dystrybucji i otrzymywania informacji, opinii i idei, co wyraźnie przyczynia się do wprowadzania innowacji, wzrostu gospodarczego i tworzenia miejsc

[11] *Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania rozporządzenia (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*, Bruksela, 14 II 2024 r., COM(2024) 64 final, s. 1.

[12] Motyw 1 rozporządzenia 2021/784. Kwestia ta została również poruszona w: *Rządowy projekt ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* – uzasadnienie, druk nr 661, s. 1, https://www.sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=661 [dostęp: 24 XII 2024].

pracy w Unii[13]. W tym kontekście zaznacza się, że to nie dostawcy usług hostingowych mogą stanowić zagrożenie w zakresie szerzenia treści o charakterze terrorystycznym, lecz ich usługi mogą być w tym celu wykorzystywane przez osoby trzecie. Zauważono jednak, że to na dostawcach usług hostingowych, ze względu na ich potencjał techniczny, spoczywają szczególne obowiązki wobec społeczeństwa w zakresie ochrony swoich usług przed wykorzystaniem przez terrorystów i udzielania pomocy w przeciwdziałaniu rozpowszechnianiu w internecie tego rodzaju treści[14]. Tym bardziej że: *Szczególnie niepokojące jest wykorzystywanie tych usług przez grupy terrorystyczne i ich zwolenników do rozpowszechniania w internecie treści o charakterze terrorystycznym w celu szerzenia ich przesłania, w celu radykalizacji i rekrutacji zwolenników oraz w celu ułatwiania działalności terrorystycznej i kierowania nią*[15].

Jeśli jednak zasady zapobiegania publikacji treści o charakterze terrorystycznym i reagowania na nią zostały uregulowane na poziomie rozporządzenia unijnego, a zatem aktu prawa mającego bezpośrednie zastosowanie we wszystkich państwach członkowskich, to w związku z § 1 ust. 1 pkt 3 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej"* (dalej: Zasady techniki prawodawczej) należy zadać pytanie, czy istniała możliwość podjęcia środków interwencji organów władzy publicznej alternatywnych w stosunku do uchwalenia ustawy. W tym przypadku odpowiedź jest prosta. Zgodnie z art. 291 ust. 1 *Traktatu o funkcjonowaniu Unii Europejskiej* państwa członkowskie są zobowiązane do podjęcia wszelkich środków prawa krajowego niezbędnych do wprowadzenia w życie prawnie wiążących aktów Unii. W art. 4 ust. 3 zdanie drugie *Traktatu o Unii Europejskiej* wskazano z kolei, że państwa członkowskie podejmują wszelkie środki ogólne lub szczególne właściwe dla zapewnienia wykonania zobowiązań wynikających z traktatów lub aktów instytucji UE. Ponadto już w samym rozporządzeniu 2021/784 zobowiązano państwa do podjęcia konkretnych działań wymagających interwencji ustawodawczej. Na przykład w art. 12 zobligowano państwa członkowskie do wyznaczenia właściwych organów w zakresie wydawania nakazów usuwania treści czy stosowania szczególnych środków zapobiegawczych. Z perspektywy krajowej natomiast, w związku z art. 7 *Konstytucji Rzeczpospolitej Polskiej z dnia*

[13] Motyw 4 rozporządzenia 2021/784.

[14] Motyw 5 rozporządzenia 2021/784.

[15] Motyw 4 zdanie 3 rozporządzenia 2021/784.

2 kwietnia 1997 r., określenie właściwości organów stanowi normę ustawową, a organy władzy publicznej działają na podstawie i w granicach prawa (zasada legalizmu). Nie budzi zatem wątpliwości potrzeba przyjęcia ustawowych rozwiązań w omawianym zakresie.

Drugim zagadnieniem ogólnym dotyczącym zapewnienia stosowania rozporządzenia 2021/784 na gruncie polskiego prawa pozostaje to, czy to zapewnienie słusznie zostało dokonane przez dodanie przepisów do ustawy o działaniach AT i czy istniały inne możliwe rozwiązania. W kontekście tych rozważań będzie pomocna krótka analiza aktualnego stanu prawnego w dziedzinie objętej regulacją, a zatem wykonanie obowiązku, o którym mowa w § 1 ust. 1 pkt 2 wspomnianych Zasad techniki prawodawczej, poprzedzającego przystąpienie do opracowania aktu prawnego.

W uzasadnieniu do ustawy o zmianie ustawy o działaniach AT i ustawy o ABW oraz AW wskazano, że tematyka rozporządzenia 2021/784 obecnie jest częściowo objęta regulacją krajową, która nie wdraża w pełni obowiązującej w tym zakresie dyrektywy 2017/541[16]. Zgodnie bowiem z jej art. 21 państwa członkowskie są zobowiązane do wprowadzenia środków, które w pierwszej kolejności zapewnią natychmiastowe usunięcie treści internetowych nawołujących do popełnienia przestępstwa terrorystycznego znajdujących się na serwerach na ich terytorium. Zgodnie z art. 21 ust. 1 dyrektywy państwa mają też podjąć działania mające doprowadzić do usunięcia takich treści znajdujących się na serwerach poza ich terytorium. Dopiero jeżeli usunięcie takich treści nie jest możliwe, państwa członkowskie mogą podjąć środki w celu zablokowania dostępu do nich (art. 21 ust. 2 dyrektywy). Polskie ustawodawstwo przewiduje zaś jedynie blokowanie treści, co w ocenie KE nie jest wystarczające do uznania implementacji za prawidłową. Brakuje podstawowego mechanizmu, który pozwalałby w pierwszej kolejności na usuwanie tych treści ze stron internetowych. W ustawie o ABW oraz AW funkcjonują bowiem przepisy, zgodnie z którymi Szef ABW, za zgodą sądu, może spowodować tzw. blokadę dostępności w internecie określonych danych powiązanych ze zdarzeniem o charakterze terrorystycznym. Zgodnie z art. 32c tej ustawy sąd 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. Może to zrobić

[16] *Rządowy projekt ustawy o zmianie ustawy*... – uzasadnienie..., s. 4.

na pisemny wniosek Szefa ABW złożony po uzyskaniu pisemnej zgody Prokuratora Krajowego. Blokada dostępności danych teleinformatycznych jest zarządzana na okres nie dłuższy niż 30 dni z możliwością jej sądowego przedłużenia na okres nie dłuższy niż trzy miesiące. Ustawa przewiduje również uproszczony tryb działania w przypadkach niecierpiących zwłoki[17]. W swoim stanowisku KE stwierdza, że:

> 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[18].

Należy także zaznaczyć, że przepisy dyrektywy 2017/541 nie zostały uchylone rozporządzeniem 2021/784, co oznacza, że oba akty są względem siebie komplementarne i powinny być stosowane równolegle. *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*[19].

Ponadto dyrektywa 2017/541 w przeciwieństwie do rozporządzenia 2021/784 nie wiąże treści o charakterze terrorystycznym z publicznym charakterem ich rozpowszechniania jako przesłanki warunkującej możliwość wydania nakazu usunięcia treści lub zablokowania dostępu do niej.

[17] Tamże

[18] *Stanowisko Komisji Europejskiej z 9 czerwca 2021 r.* (sygn. INFR(2021)2046, C(2021)3630 final), s. 7; *Rządowy projekt ustawy o zmianie ustawy...* – uzasadnienie..., s. 15.

[19] *Rządowy projekt ustawy o zmianie ustawy...* – uzasadnienie..., s. 14.

Na bazie dyrektywy można więc dążyć do usuwania treści np. w ramach forów internetowych o ograniczonej dostępności.

W rezultacie, chociaż wskazany przepis ustawy o ABW oraz AW dotyczy kwestii blokowania treści w internecie, to nie może być utożsamiany z obowiązkami regulacyjnymi związanymi z zapewnieniem stosowania rozporządzenia 2021/784. W związku z tym utrzymano w mocy art. 32c ustawy o ABW oraz AW, ale przeprowadzono jego modyfikację, zgodnie z którą ten przepis ma zastosowanie w przypadkach publikowania lub prób publikowania w internecie treści o charakterze terrorystycznym przez podmioty niebędące dostawcami usług hostingowych w rozumieniu rozporządzenia 2021/784.

Skoro jednak dotychczasowe regulacje znajdowały się w ustawie o ABW oraz AW, to warto się zastanowić, czy nowe regulacje, zbieżne tematycznie, również nie powinny znaleźć się w tej ustawie. W opinii autora pozytywna odpowiedź na to pytanie budzi istotne wątpliwości. Owszem, zapewnienie stosowania rozporządzenia 2021/784 wymaga wyznaczenia właściwego organu po stronie państwa członkowskiego. Jeśli w przypadku Polski zdecydowano, że będzie nim Szef ABW, to wskazanie to mogłoby nastąpić w ustawie pragmatycznej określającej zadania i uprawnienia tej służby oraz jej organy, czyli w ustawie o ABW oraz AW. Zakres spraw przekazanych przez unijnego prawodawcę do uregulowania na poziomie krajowym jest jednak znacznie szerszy. Rozporządzenie 2021/784 określa bowiem nie tylko sferę działania organów właściwych, lecz także prawa, w tym do zaskarżenia decyzji organów państwowych, i obowiązki dostawców usług hostingowych i dostawców treści oraz system i wymiar kar możliwych do nałożenia na nich. Jest to zatem zakres znacznie wykraczający poza sferę, która może być normowana w ustawie pragmatycznej dotyczącej danej formacji. Ustawy pragmatyczne nie powinny, choć obecnie się to zdarza, regulować praw i obowiązków innych podmiotów. Co więcej, w opinii autora należy uznać za wątpliwe pod względem legislacyjnym dotychczasowe umiejscowienie przepisów art. 32c ustawy o ABW oraz AW. Przepisy te zostały wprowadzone przepisami zmieniającymi w ramach pierwotnego tekstu ustawy o działaniach AT w 2016 r., zatem już wtedy ustawodawca mógł je umieścić w tej ustawie. Inna decyzja prawdopodobnie była podyktowana tym, że konstrukcja przepisów w wymiarze proceduralnym jest zbliżona do instytucji prawnej kontroli operacyjnej unormowanej w art. 27 ustawy o ABW oraz AW (analogicznie jak w przypadku ustaw pragmatycznych innych służb uprawnionych do

jej prowadzenia, np. w art. 19 ustawy o Policji). Zatem to nie przepisy zapewniające stosowanie rozporządzenia 2021/784 powinny znaleźć się w ustawie o ABW oraz AW, lecz odwrotnie – to dotychczasowe przepisy związane z blokowaniem treści ujętej w tej ustawie mogłyby docelowo znaleźć się w ustawie o działaniach AT. Na marginesie warto zauważyć, że uwaga ta odnosi się również do art. 32a–32b ustawy o ABW oraz AW dotyczących prowadzenia przez ABW oceny bezpieczeństwa systemów teleinformatycznych organów administracji publicznej i operatorów infrastruktury krytycznej, a także systemów ostrzegania.

Kolejnego argumentu potwierdzającego słuszność ujęcia przepisów związanych z rozporządzeniem 2021/784 dostarcza § 2 Zasad techniki prawodawczej, zgodnie z którym ustawa powinna wyczerpująco regulować daną dziedzinę spraw i nie pozostawiać poza zakresem swego unormowania istotnych fragmentów tej dziedziny. W kontekście związanym z problematyką zagrożeń o charakterze terrorystycznym podstawową regulacją jest ustawa o działaniach AT i to w niej co do zasady powinny zawierać się zagadnienia związane z tą problematyką. Ten argument jest adekwatny również w odniesieniu do drugiej potencjalnej alternatywnej lokalizacji przepisów służących stosowaniu rozporządzenia 2021/784, tj. do unormowania tej kwestii w nowej odrębnej regulacji.

Na marginesie warto zauważyć, że z analogicznych powodów do ustawy o działaniach AT mogłyby zostać włączone przepisy obecnej *Ustawy z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych,* która służy stosowaniu *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 98/2013 z dnia 15 stycznia 2013 r. w sprawie wprowadzania do obrotu i używania prekursorów materiałów wybuchowych*. Zostało ono wydane w następstwie zamachów przeprowadzonych przez norweskiego ekstremistę Andersa Breivika na siedzibę premiera Norwegii oraz na uczestników obozu młodzieżówki norweskiej Partii Pracy[20].

[20] Zob. szerzej: M. Cichomski, P. Marchliński, *Krajowe rozwiązania w zakresie bezpieczeństwa obrotu prekursorami materiałów wybuchowych – po zamachu terrorystycznym w Norwegii 22 lipca 2011 r. w kontekście nowych zadań Policji*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, s. 591–600.

Podstawowe rozwiązania zawarte w rozporządzeniu 2021/784 w związku z przeciwdziałaniem rozpowszechnianiu w internecie treści o charakterze terrorystycznym – nakazy usunięcia i środki szczególne

W kontekście komentarza do poszczególnych przepisów ustawy o działaniach AT są konieczne liczne odwołania do przepisów i motywów rozporządzenia 2021/784, ale służą one wykładni poszczególnych przepisów polskiego prawa. Niezbędne jest jednak syntetyczne przedstawienie podstawowych instrumentów zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, wprowadzanych rozporządzeniem 2021/784. Umożliwienie ich stosowania w Polsce to cel działań na poziomie krajowego ustawodawcy.

Na potrzeby tego opracowania można wyróżnić dwa podstawowe mechanizmy przeciwdziałania rozpowszechnianiu w internecie wspomnianych treści:

- 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 (dalej: nakazy usunięcia);
- wydawanie decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, na podstawie art. 5 rozporządzenia 2021/784 (dalej: środki szczególne).

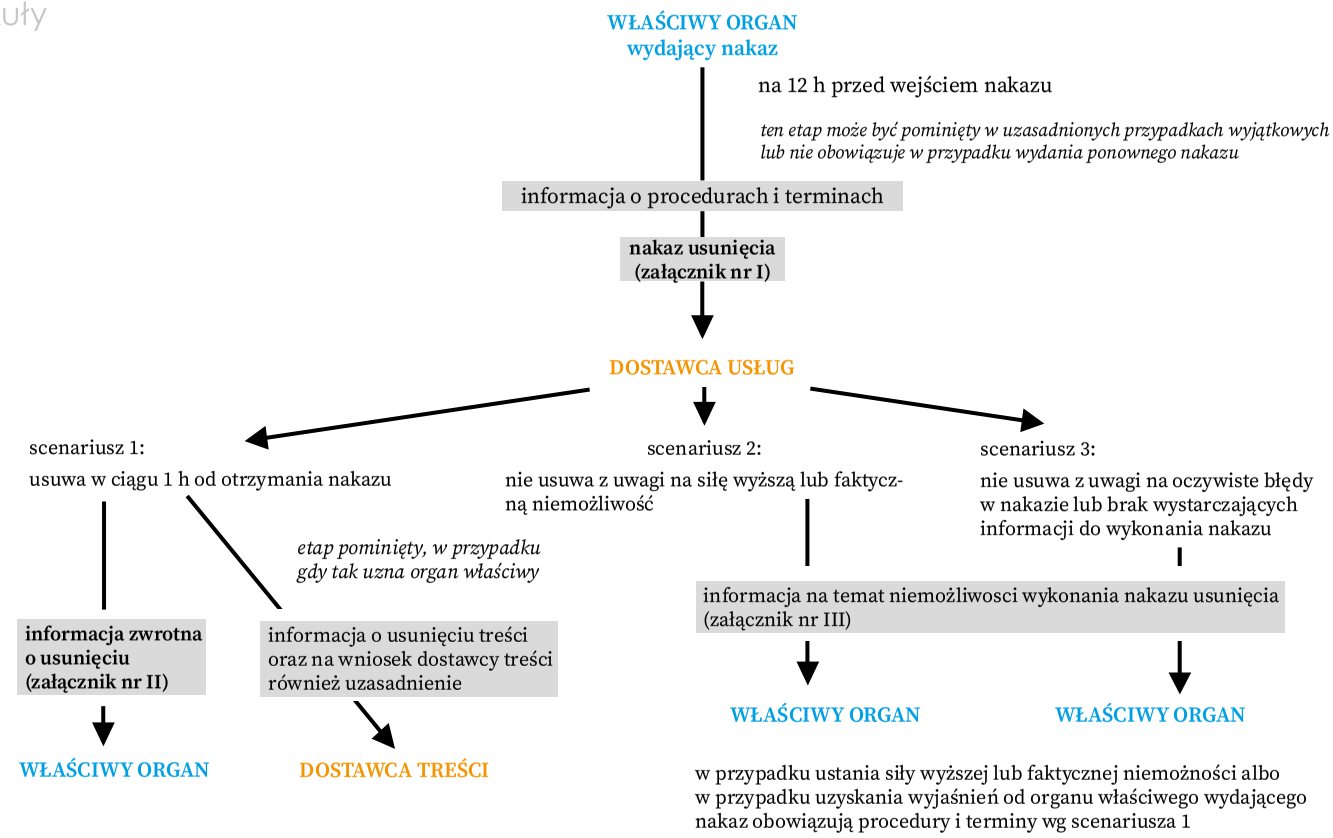
Tym dwóm wskazanym instrumentom odpowiada szereg dodatkowych uprawnień i przepisów proceduralnych, a także mechanizmów i narzędzi współpracy między państwami UE, KE i Agencją Unii Europejskiej ds. Współpracy Organów Ścigania, czyli Europolem, a także dostawcami usług hostingowych (schematy 1 i 2).

Pierwszy z wymienionych instrumentów – nakaz usunięcia – zakłada, że właściwy organ każdego państwa członkowskiego jest uprawniony do wydania nakazu usunięcia zobowiązującego dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści terrorystycznych we wszystkich państwach członkowskich. W następstwie wydanego nakazu dostawcy usług hostingowych jak najszybciej, nie później niż w ciągu jednej godziny od otrzymania nakazu usunięcia, usuwają treści lub uniemożliwiają do nich dostęp we wszystkich państwach członkowskich.

Nakazy są wydawane na ujednoliconym formularzu i zawierają takie informacje, jak: dane identyfikacyjne właściwego organu wydającego nakaz, uzasadnienie, dokładny ujednolicony format adresowania zasobów (adres URL) oraz, w razie potrzeby, dodatkowe informacje służące identyfikacji treści o charakterze terrorystycznym czy informację na temat środków zaskarżenia przysługujących dostawcy usług hostingowych i dostawcy treści. Następnie dostawcy usług hostingowych informują właściwy organ o wykonaniu nakazu – wskazują zwłaszcza czas usunięcia lub uniemożliwienia dostępu do treści (wzór nakazu usunięcia został określony w załączniku I do rozporządzenia 2021/784).

Jeżeli w odniesieniu do danego dostawcy usług hostingowych taki nakaz jest wydawany po raz pierwszy, to poprzedza go udzielenie temu dostawcy informacji o mających zastosowanie procedurach i terminach co najmniej 12 godzin przed wydaniem nakazu usunięcia. Obowiązek ten może zostać pominięty w szczególnie uzasadnionych przypadkach.

Jeżeli dostawca usług hostingowych nie jest w stanie wykonać nakazu ze względu na siłę wyższą lub faktyczną niemożliwość, których nie można przypisać temu dostawcy, w tym z przyczyn technicznych lub operacyjnych, dających się obiektywnie uzasadnić, informuje o tym właściwy organ, który wydał nakaz, a godzinny termin na usunięcie treści lub zablokowanie dostępu do niej zaczyna biec od momentu, gdy ustaną ww. powody. Jeżeli natomiast dostawca usług hostingowych nie jest w stanie wykonać nakazu, ponieważ zawiera on błędy lub nie zawiera informacji wystarczających do jego wykonania, informuje o tym właściwy organ, który wydał nakaz usunięcia. W tym wypadku termin zaczyna biec od momentu, gdy dostawca usług hostingowych otrzymał niezbędne wyjaśnienia. Nakaz staje się ostateczny po upływie terminu do wniesienia środka zaskarżenia, w przypadku gdy nie został on wniesiony zgodnie z prawem krajowym albo na skutek utrzymania nakazu usunięcia w wyniku wniesienia środka zaskarżenia.



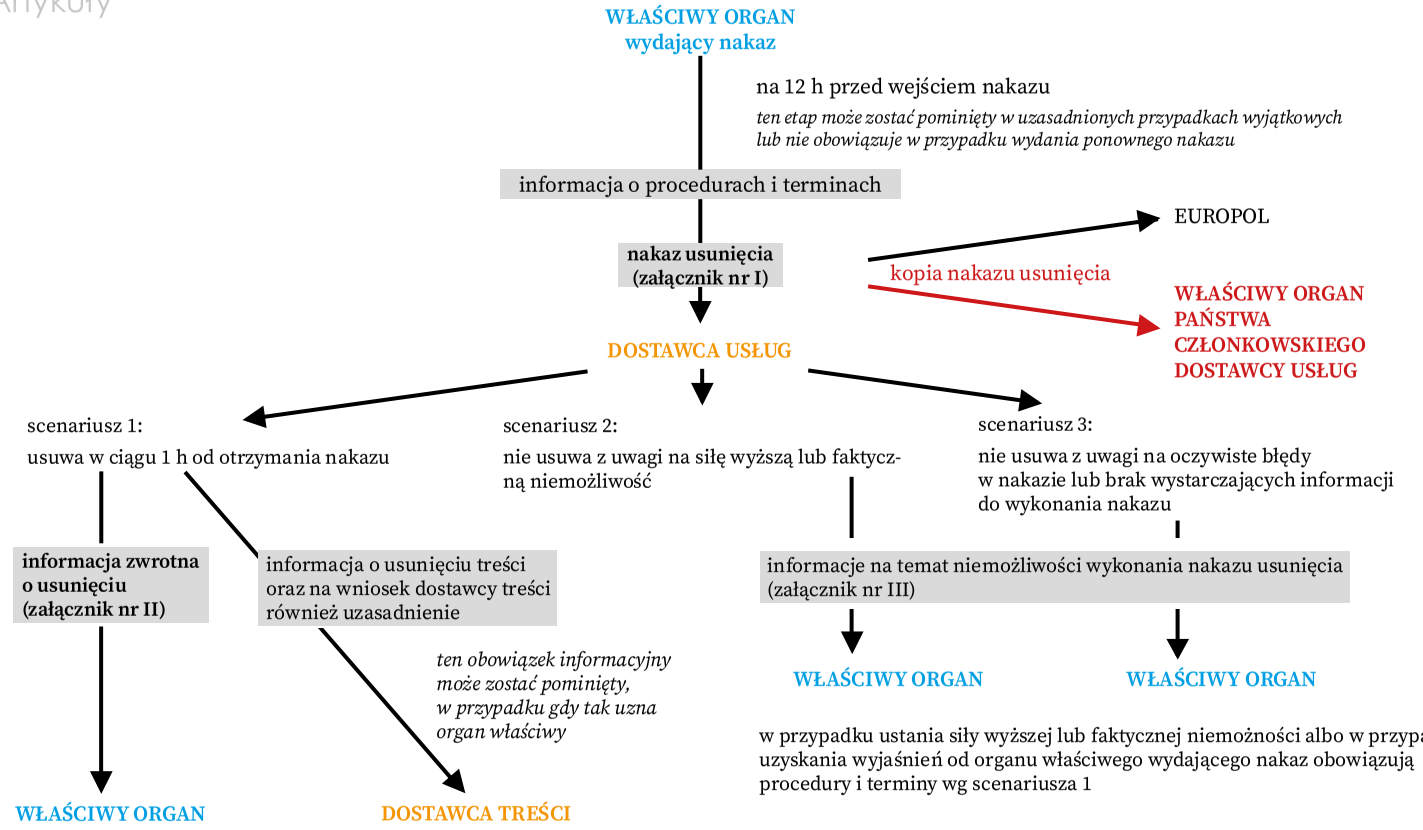
Schemat 1. Procedura nałożenia nakazu usunięcia treści o charakterze terrorystycznym, w przypadku gdy główna jednostka organizacyjna lub przedstawiciel prawny dostawcy usług hostingowych znajduje się na terenie tego samego państwa członkowskiego co właściwy organ wydający nakaz.

Źródło: opracowanie Anety Sudy, *Mechanizmy blokowania w internecie treści o charakterze terrorystycznym w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*, prezentacja Ministerstwa Spraw Wewnętrznych i Administracji przygotowana na potrzeby Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych.

Należy wspomnieć o mechanizmie weryfikowania nakazów usunięcia wydanych przez właściwe organy innych państw członkowskich oraz stwierdzania ewentualnych naruszeń w tym zakresie (art. 4 rozporządzenia 2021/784). Jest to tzw. procedura dotycząca transgranicznych nakazów usunięcia (schemat 3). Zgodnie z tym rozwiązaniem w przypadku, gdy dostawca usług hostingowych nie ma głównej jednostki organizacyjnej ani przedstawiciela prawnego w państwie członkowskim właściwego organu, który wydał nakaz, organ ten przekazuje kopię nakazu usunięcia właściwemu organowi państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę.

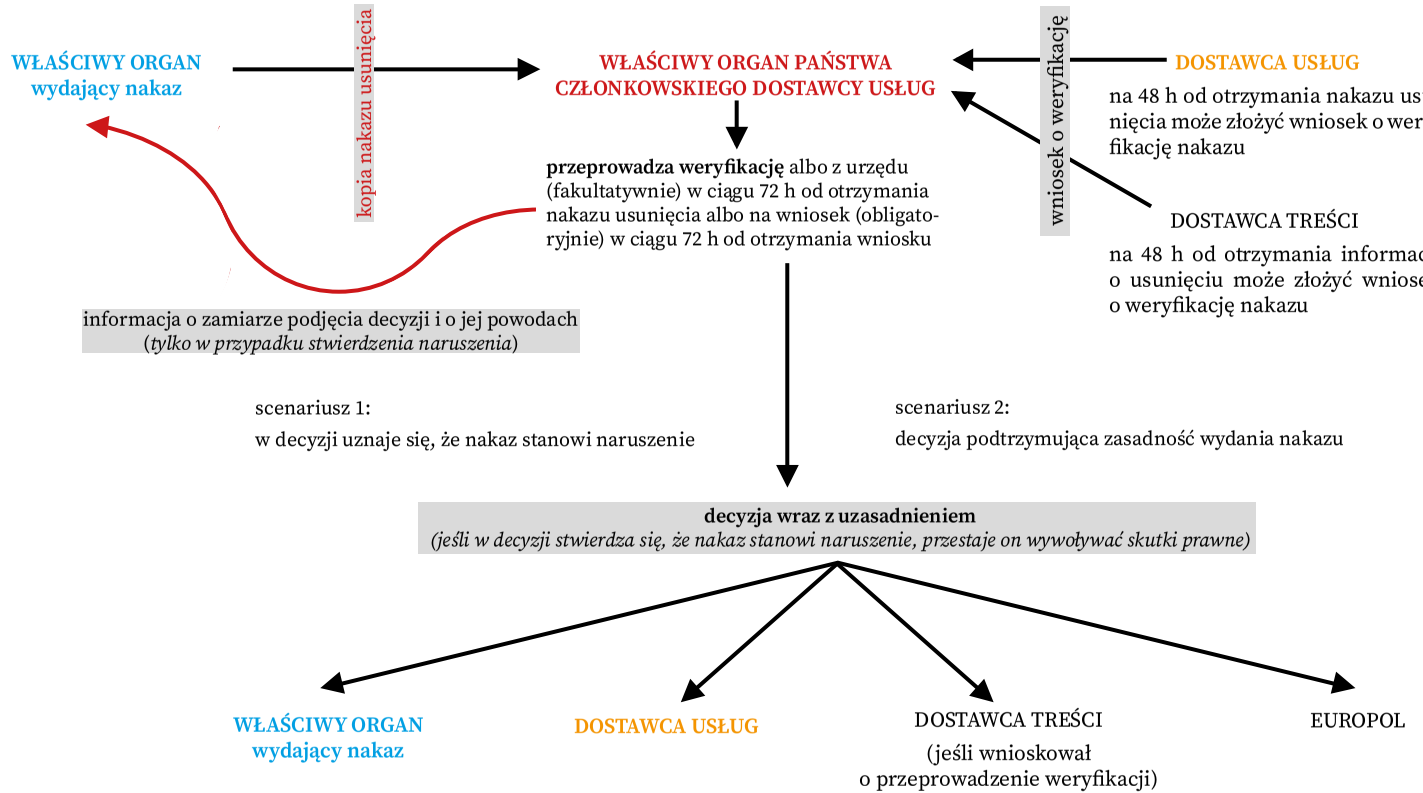
Właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, może z własnej inicjatywy, w ciągu 72 godzin od otrzymania kopii tego nakazu dokonać jego weryfikacji, aby ustalić, czy nie narusza on w sposób poważny lub oczywisty podstaw prawnych jego wydania lub praw podstawowych i wolności. W przypadku stwierdzenia takiego naruszenia podejmuje w tej sprawie decyzję wraz z uzasadnieniem, w tym samym terminie.

Również dostawcy usług hostingowych i dostawcy treści mają możliwość zainicjowania działań weryfikacyjnych – w ciągu 48 godzin od otrzymania nakazu mogą wystąpić z wnioskiem o przeprowadzenie weryfikacji do właściwego organu państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę. Weryfikacja ta jest przeprowadzana w ciągu 72 godzin od otrzymania wniosku. W jej wyniku właściwy organ podejmuje decyzję, której wydanie jest poprzedzone przekazaniem informacji do organu wydającego nakaz o zamiarze jej podjęcia. W przypadku podjęcia decyzji organ ten niezwłocznie powiadamia o niej właściwy organ, który wydał nakaz usunięcia, dostawcę usług hostingowych, dostawcę treści, który wystąpił o przeprowadzenie weryfikacji, oraz Europol. W przypadku gdy stwierdza się, że nakaz usunięcia stanowi naruszenie, przestaje on wywoływać skutki prawne, a dostawca usług hostingowych natychmiast przywraca dane treści lub dostęp do nich.



Schemat 2. Procedura nałożenia nakazu usunięcia treści o charakterze terrorystycznym, w przypadku gdy główna jednostka organizacyjna lub przedstawiciel prawny dostawcy usług hostingowych nie znajduje się na terenie tego samego państwa członkowskiego co właściwy organ wydający nakaz.

Źródło: opracowanie Anety Sudy, *Mechanizmy blokowania w internecie treści o charakterze terrorystycznym w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*, prezentacja Ministerstwa Spraw Wewnętrznych i Administracji przygotowana na potrzeby Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych.



Schemat 3. Procedura nałożenia transgranicznego nakazu usunięcia.

Źródło: opracowanie Anety Sudy, *Mechanizmy blokowania w internecie treści o charakterze terrorystycznym w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*, prezentacja Ministerstwa Spraw Wewnętrznych i Administracji przygotowana na potrzeby Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych.

Drugi z wyróżnionych podstawowych mechanizmów zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym i reagowaniem na te incydenty (środki szczególne) to wydawanie decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym oraz nadzoru nad wdrażaniem przez nich środków szczególnych.

Tłumacząc *ratio legis* tego rozwiązania, unijny ustawodawca wskazał, że:

> W celu zmniejszenia dostępności treści o charakterze terrorystycznym w ramach świadczonych przez siebie usług dostawcy usług hostingowych narażeni na takie treści powinni wdrożyć środki szczególne, uwzględniając ryzyko i poziom narażenia na treści o charakterze terrorystycznym, a także wpływ na prawa osób trzecich oraz interes publiczny w zakresie informacji. Dostawcy usług hostingowych powinni ustalić, jakie odpowiednie, skuteczne i proporcjonalne środki szczególne powinny zostać wdrożone, by identyfikować i usuwać treści o charakterze terrorystycznym. Środki szczególne mogą obejmować odpowiednie techniczne lub operacyjne środki lub zdolności, takie jak personel lub środki techniczne, do celów identyfikowania i niezwłocznego usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich, mechanizmy umożliwiające użytkownikom zgłaszanie lub sygnalizowanie domniemanych treści o charakterze terrorystycznym lub inne środki, które dostawca usług hostingowych uzna za odpowiednie i skuteczne w celu przeciwdziałania dostępności, w ramach jego usług, treści o charakterze terrorystycznym[21].

Dostawca usług hostingowych uznany za dostawcę narażonego na treści o charakterze terrorystycznym zamieszcza w swoich warunkach umownych oraz stosuje postanowienia mające przeciwdziałać wykorzystywaniu jego usług do publicznego rozpowszechniania treści o charakterze terrorystycznym i podejmuje w tym celu środki szczególne. Mogą to być np.:

- techniczne i operacyjne środki lub zdolności, takie jak odpowiedni personel lub środki techniczne do celów identyfikowania i niezwłocznego usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich;
- łatwo dostępne i przyjazne dla użytkownika mechanizmy umożliwiające użytkownikom zgłaszanie lub sygnalizowanie dostawcy

[21] Motyw 22 rozporządzenia 2021/784.

usług hostingowych domniemanych treści o charakterze terrorystycznym;
- inne mechanizmy zwiększające świadomość na temat dostępności treści o charakterze terrorystycznym w ramach świadczonych przez niego usług, takie jak mechanizmy służące moderowaniu użytkowników;
- inne środki, które dostawca usług hostingowych uzna za stosowne, by przeciwdziałać dostępności treści o charakterze terrorystycznym w ramach świadczonych przez niego usług.

Zgodnie z założeniem środki szczególne mają skutecznie zmniejszać poziom narażenia usług dostawcy usług hostingowych na treści o charakterze terrorystycznym, być ukierunkowane i proporcjonalne, a także stosowane w sposób staranny i niedyskryminacyjny, uwzględniający pełne poszanowanie praw i uzasadnionego interesu użytkowników.

Dostawcę usług hostingowych należy uznać za narażonego na treści o charakterze terrorystycznym w przypadku, gdy właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, podjął decyzję, że ten dostawca jest narażony na treści o charakterze terrorystycznym. Ta decyzja powinna zostać podjęta na podstawie obiektywnych czynników, takich jak otrzymanie przez dostawcę w ciągu ostatnich 12 miesięcy co najmniej dwóch ostatecznych nakazów usunięcia tego rodzaju treści.

Po otrzymaniu decyzji dostawca usług hostingowych w terminie trzech miesięcy powiadamia właściwy organ o środkach szczególnych, które podjął lub które zamierza podjąć w celu zapewnienia wykonania ciążących na nim obowiązków. Następnie raz do roku dostawca usług hostingowych sporządza sprawozdanie z ich realizacji.

Jeżeli właściwy organ uzna, że podjęte środki szczególne nie są zgodne z wymogami, kieruje do dostawcy usług hostingowych decyzję zobowiązującą go do podjęcia niezbędnych środków. Dostawca usług hostingowych może wybrać, jaki rodzaj środków szczególnych podejmie. Może również w dowolnym momencie zwrócić się do właściwego organu o dokonanie przeglądu oraz, w stosownych przypadkach, o zmianę lub uchylenie decyzji o uznaniu go za dostawcę usług hostingowych narażonego na treści o charakterze terrorystycznym.

Na koniec tej części artykułu warto przywołać kilka danych statystycznych dotyczących stosowania rozporządzenia 2021/784 do 31 grudnia

2023 r.[22] Zgodnie z ustaleniami KE państwa członkowskie wydały 349 nakazów usunięcia treści o charakterze terrorystycznym. Z tej możliwości skorzystały organy właściwe sześciu państw członkowskich, tj. Hiszpanii – 62 nakazy, Rumunii – 2 nakazy, Francji – 26 nakazów, Niemiec – 249 nakazów (wszystkie wydane po ataku przeprowadzonym przez Hamas 7 października 2023 r.), Czech – 2 nakazy, Austrii – 8 nakazów. Nakazy były kierowane m.in. do następujących podmiotów: Telegram, Meta, JustPaste.it, TikTok, DATA ROOM S.R.L., FlokiNET S.R.L., Archive.org, SoundCloud, X, Jumpshare, KrakenFiles.com, Top4toP oraz Catbox.

Na 349 wydanych nakazów usunięcia tylko w 10 przypadkach dostawca usług hostingowych nie usunął treści o charakterze terrorystycznym lub nie zablokował ich w maksymalnym terminie, tj. do jednej godziny od otrzymania nakazu. Tylko w jednym przypadku dostawca usług hostingowych stwierdził, że wykonanie nakazu jest niemożliwe.

Żaden nakaz nie podlegał weryfikacji w procedurze dotyczącej transgranicznych nakazów usunięcia. W związku z tym nie odnotowano przypadku stwierdzającego, że wydany nakaz dokonał takiego naruszenia.

Dotychczas żaden z dostawców usług hostingowych nie został określony jako narażony na treści o charakterze terrorystycznym, a zatem żaden z dostawców nie był zobowiązany do wdrożenia środków szczególnych.

Co warte odnotowania, żaden wydany nakaz nie został dotychczas zaskarżony do sądu.

Komentarz do poszczególnych przepisów ustawy o działaniach AT w związku z zapobieganiem rozpowszechnianiu w internecie treści o charakterze terrorystycznym

Ustawą o zmianie ustawy o działaniach AT i ustawy o ABW oraz AW wprowadzono do ustawy o działaniach AT dwie grupy przepisów. Pierwsza z nich to poszerzenie słownika ustawowego, zawartego w art. 2 znowelizowanej ustawy, o trzy definicje, z których każda zawiera odwołanie do rozporządzenia 2021/784. Druga grupa przepisów została objęta nową jednostką systematyki ustawowej oznaczoną jako rozdział 5a – przeciwdziałanie rozpowszechnianiu w internecie treści o charakterze terrorystycznym. Zawarto w nim sześć przepisów związanych z wyznaczeniem właściwego organu po

[22] Na podstawie *Sprawozdania Komisji z wykonania rozporządzenia (UE) 2021/784...*

stronie krajowej, przepisy proceduralne i przepisy określające kary administracyjne, czyli normy prawne bezpośrednio zapewniające stosowanie rozporządzenia 2021/784. Ponadto uzupełniono tytuł ustawy o odesłanie do tego rozporządzenia.

Kolejna część artykułu to komentarz do poszczególnych przepisów.

> Art. 1. W ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2024 r. poz. 92 i 1248) wprowadza się następujące zmiany:
>
> 1) do tytułu ustawy dodaje się odnośnik w brzmieniu:
>
> „1) Niniejsza ustawa służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79)".

Przez uzupełnienie tytułu ustawy o działaniach antyterrorystycznych o odnośnik do stosowania rozporządzenia 2021/784 zrealizowano obowiązek wynikający z § 19a ust. 2 Zasad techniki prawodawczej. Zgodnie z nim w przypadku ustawy, której uchwalenie jest związane z wydaniem lub obowiązywaniem aktu normatywnego ustanowionego przez instytucję UE dającego się bezpośrednio stosować, po określeniu przedmiotu ustawy zamieszcza się odnośnik do tytułu ustawy informujący o akcie normatywnym, z którym ustawa jest związana, co wyraża się w szczególności zwrotem „niniejsza ustawa służy stosowaniu... [tytuł aktu]".

> 2) w art. 2 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8–10 w brzmieniu:
>
> [ilekroć w ustawie jest mowa o:]
>
> „8) dostawcy usług hostingowych – należy przez to rozumieć dostawcę usług polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek, o którym mowa w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79), zwanego dalej „rozporządzeniem 2021/784"; (...)

Zgodnie z art. 2 pkt 1 rozporządzenia 2021/784 „dostawca usług hostingowych" oznacza dostawcę usług (zdefiniowanych w art. 1 lit. b *Dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego*), polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek. Zgodnie ze wskazaną dyrektywą „usługa" oznacza każdą usługę społeczeństwa informacyjnego, to znaczy każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Z tym że „na odległość" oznacza, że usługa jest świadczona bez równoczesnej obecności stron. „Drogą elektroniczną" oznacza, że usługa jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych. „Na indywidualne żądanie odbiorcy usług" oznacza, że usługa jest świadczona przez przesyłanie danych na indywidualne żądanie.

Warto zwrócić uwagę na motyw 13 przywoływanego rozporządzenia, zgodnie z którym:

> Aby w skuteczny sposób przeciwdziałać rozpowszechnianiu w internecie treści o charakterze terrorystycznym, a jednocześnie zapewniać poszanowanie życia prywatnego osób, niniejsze rozporządzenie powinno mieć zastosowanie do dostawców usług społeczeństwa informacyjnego, którzy przechowują i publicznie rozpowszechniają informacje i materiały dostarczone przez użytkownika usługi na jego wniosek, nawet jeżeli przechowywanie i publiczne rozpowszechnianie takich informacji i materiałów ma charakter czysto techniczny, automatyczny i bierny. Pojęcie „przechowywania" należy rozumieć jako przechowywanie danych w pamięci fizycznego lub wirtualnego serwera. Dostawcy usług „zwykłego przekazu" lub „cachingu" oraz innych usług świadczonych w innych warstwach infrastruktury internetowej, które nie obejmują przechowywania, takie jak rejestry i rejestratorzy, a także dostawcy usług DNS (system nazw domen), usług płatniczych lub usług ochrony przed atakami typu DDoS (rozproszony atak typu „odmowa usługi") nie powinni zatem być objęci zakresem stosowania niniejszego rozporządzenia.

Rozporządzenie 2021/784 zakresem swej regulacji objęło dostawców usług hostingowych oferujących usługi w UE, tj. umożliwiających osobom fizycznym lub prawnym w co najmniej jednym państwie członkowskim korzystanie z usług dostawcy usług hostingowych, którego łączy z danym państwem członkowskim istotny związek wynikający z posiadania przez niego jednostki organizacyjnej w Unii, albo ze szczególnych kryteriów faktycznych, takich jak posiadanie przez dostawcę znacznej liczby użytkowników jego usług w co najmniej jednym państwie członkowskim lub kierowanie jego działalności do co najmniej jednego państwa członkowskiego (art. 2 pkt 4 i 5 rozporządzenia). Oferowanie usług musi być prowadzone w zakresie, w jakim dostawcy usług hostingowych publicznie rozpowszechniają informacje (art. 1 ust. 2 tego rozporządzenia), bez względu na umiejscowienie ich głównej jednostki organizacyjnej, tj. siedziby głównej lub siedziby statutowej, w której są wykonywane główne funkcje finansowe i jest sprawowana kontrola operacyjna (art. 2 pkt 9 rozporządzenia). Należy jednak pamiętać, że w przypadku gdy dostęp do informacji wymaga rejestracji lub dopuszczenia do udziału w grupie użytkowników – zgodnie z art. 2 pkt 3 i motywem 14 rozporządzenia – informacje te należy uznawać za publicznie rozpowszechniane jedynie wtedy, gdy użytkownicy poszukujący dostępu do informacji są automatycznie rejestrowani lub dopuszczani do udziału w grupie użytkowników, bez konieczności podejmowania przez człowieka decyzji, komu przyznać taki dostęp.

W celu zapewnienia realnego stosowania rozporządzenia w odniesieniu do dostawców usług hostingowych na podstawie art. 17 rozporządzenia 2021/784 wprowadzono obowiązek, zgodnie z którym, jeżeli dostawca nie ma głównej jednostki organizacyjnej w UE, to wyznacza na piśmie osobę fizyczną lub prawną jako swojego przedstawiciela prawnego w Unii do celów odbioru, stosowania się do i wykonywania nakazów usunięcia i decyzji wydanych przez właściwe organy. Co więcej, przekazuje on swojemu przedstawicielowi prawnemu uprawnienia i zasoby niezbędne do stosowania się do tych nakazów usunięcia i decyzji oraz do współpracy z właściwymi organami. Dostawca usług hostingowych powiadamia o wyznaczeniu przedstawiciela prawnego właściwy organ państwa członkowskiego, w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, a także udostępnia publicznie informacje na temat przedstawiciela prawnego. Przedstawiciel prawny może zostać pociągnięty do odpowiedzialności z tytułu naruszeń niniejszego rozporządzenia, bez uszczerbku dla odpowiedzialności dostawcy usług hostingowych i działań prawnych przeciwko dostawcy usług hostingowych.

Wspomniana kwestia, w opinii autora, ma kluczowe znaczenie dla efektywności stosowania samego rozporządzenia 2021/784 z perspektywy skuteczności usuwania lub blokowania treści o charakterze terrorystycznym. W przeciwieństwie bowiem do rozwiązań przyjmowanych na poziomie poszczególnych państw, w tym obowiązujących w Polsce mechanizmów określonych w ustawie o ABW oraz AW, daje się ono skutecznie zastosować względem treści zamieszczanych u dostawcy usług hostingowych znajdującego się poza danym państwem. Analogiczną opinię wyraziła KE:

> Chociaż dobrowolne środki i niewiążące zalecenia przyczyniły się do ograniczenia dostępności w internecie treści o charakterze terrorystycznym, ze względu na pewne wyzwania – w tym ze względu na fakt, że niewielu dostawców usług hostingowych wprowadziło mechanizmy dobrowolne[23], a także ze względu na rozdrobnienie przepisów proceduralnych w poszczególnych państwach członkowskich – skuteczność i efektywność współpracy między państwami członkowskimi a dostawcami usług hostingowych była ograniczona, w związku z czym zaistniała konieczność ustanowienia środków regulacyjnych[24]. W związku z tym skuteczne stosowanie rozporządzenia ma kluczowe znaczenie dla przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym. Komisja aktywnie wspierała właściwe organy krajowe w tym procesie[25].

2) w art. 2 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8–10 w brzmieniu: […]
[ilekroć w ustawie jest mowa o:]
„9) dostawcy treści – należy przez to rozumieć użytkownika, o którym mowa w art. 2 pkt 2 rozporządzenia 2021/784;"

Zgodnie z art. 2 pkt 2 rozporządzenia 2021/784 „dostawca treści" oznacza użytkownika, który dostarczył informacje, które są lub były przechowywane i publicznie rozpowszechniane przez dostawcę usług hostingowych.

[23] *Commission Staff Working Document Impact Assessment. Accompanying the document. Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online*, Brussels, 12 IX 2018 r., SWD(2018) 408 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN [dostęp: 4 V 2023].

[24] Tamże.

[25] *Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania rozporządzenia (UE) 2021/784…*, s. 4.

„Publiczne rozpowszechnianie" oznacza natomiast udostępnianie informacji, na wniosek dostawcy treści, potencjalnie nieograniczonej liczbie osób (art. 2 pkt 3 rozporządzenia 2021/784).

O ile unijny prawodawca wyraźnie podkreśla kluczową w wymiarze społecznym i gospodarczym rolę dostawców usług hostingowych jako łączników pomiędzy przedsiębiorstwami i obywatelami ustanawiających przestrzeń do publicznej debaty czy wymiany informacji, a których działalność może być wykorzystana przez osoby trzecie do przekazywania treści o charakterze terrorystycznym, o tyle w odniesieniu do dostawcy treści wskazuje się wprost, że ponosi on odpowiedzialność redakcyjną za swoją działalność.

2) w art. 2 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8–10 w brzmieniu: […]
[ilekroć w ustawie jest mowa o:]
10) treściach o charakterze terrorystycznym – należy przez to rozumieć materiały, o których mowa w art. 2 pkt 7 rozporządzenia 2021/784.

Zgodnie z art. 2 pkt 7 rozporządzenia 2021/784 treści o charakterze terrorystycznym oznaczają materiały, które:

- podżegają do popełnienia jednego z przestępstw, o których mowa w art. 3 ust. 1 lit. a–i dyrektywy 2017/541 (wskazane poniżej), w przypadku gdy takie materiały, bezpośrednio lub pośrednio, np. przez pochwalanie aktów terrorystycznych, popierają popełnianie przestępstw terrorystycznych i tym samym stwarzają niebezpieczeństwo popełnienia jednego lub większej liczby takich przestępstw;
- nakłaniają osobę lub grupę osób do popełnienia lub przyczynienia się do popełnienia jednego z niżej wskazanych przestępstw w rozumieniu dyrektywy 2017/541;
- 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 jednego z niżej wymienionych przestępstw w rozumieniu dyrektywy 2017/541;

– stwarzają zagrożenie popełnienia jednego z niżej wskazanych przestępstw w rozumieniu dyrektywy 2017/541.

Zgodnie z art. 3 ust. 1 lit. a-j dyrektywy 2017/541 przestępstwa o charakterze terrorystycznym to czyny umyślne, określone zgodnie z polskim prawem jako przestępstwa, które ze względu na swój charakter lub kontekst mogą wyrządzić poważne szkody państwu lub organizacji międzynarodowej i zostały popełnione w określonym celu. Są to:

a) ataki na życie ludzkie, które mogą powodować śmierć;
b) ataki na integralność fizyczną osoby;
c) porwania lub branie zakładników;
d) spowodowanie rozległych zniszczeń obiektów rządowych lub obiektów użyteczności publicznej, systemu transportowego, infrastruktury, w tym systemu informacyjnego, stałych platform umieszczonych na szelfie kontynentalnym, miejsca publicznego lub mienia prywatnego – jeżeli zniszczenia te mogą zagrozić życiu ludzkiemu lub spowodować poważne straty gospodarcze;
e) zajęcie statku powietrznego, statku wodnego lub innego środka transportu publicznego lub towarowego;
f) wytwarzanie, posiadanie, nabywanie, przewożenie, dostarczanie lub używanie materiałów wybuchowych lub broni, w tym broni chemicznej, biologicznej, radiologicznej lub jądrowej, jak również badania nad taką bronią i jej rozwój;
g) uwalnianie substancji niebezpiecznych lub powodowanie pożarów, powodzi lub wybuchów, czego rezultatem jest zagrożenie życia ludzkiego;
h) zakłócanie lub przerywanie dostaw wody, energii elektrycznej lub wszelkich innych podstawowych zasobów naturalnych, czego rezultatem jest zagrożenie życia ludzkiego;
i) niezgodna z prawem ingerencja w systemy, o której mowa w art. 4 dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE (1), w przypadkach gdy zastosowanie ma art. 9 ust. 3 lub art. 9 ust. 4 lit. b) lub c) tej dyrektywy, oraz niezgodna z prawem ingerencja w dane, o której mowa w art. 5 tej dyrektywy, w przypadkach gdy zastosowanie ma art. 9 ust. 4 lit. c) tej dyrektywy[26];

[26] Zgodnie z art. 4 i 5 *Dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW*, niezgodna z prawem ingerencja w systemy informatyczne polega na wprowadzeniu, przekazywaniu, uszkadzaniu, usuwaniu, pogarszaniu, zmienianiu lub

j) grożenie popełnieniem jednego z wymienionych czynów.

Zgodnie z art. 3 ust. 2 dyrektywy 2017/541 wskazane kategorie przestępstw są przestępstwami terrorystycznymi, jeżeli zostały popełnione w celu:

- poważnego zastraszenia ludności;
- bezprawnego zmuszenia rządu lub organizacji międzynarodowej do podjęcia lub zaniechania jakiegoś działania;
- poważnej destabilizacji lub zniszczenie podstawowych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych danego państwa lub danej organizacji międzynarodowej.

Przytoczona definicja, co do zasady, odpowiada definicji przestępstwa o charakterze terrorystycznym zawartej w art. 115 § 20 *Ustawy z dnia 6 czerwca 1997 r. Kodeks karny*, zgodnie z którą przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:

1) poważnego zastraszenia wielu osób,
2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
3) wywołania poważnych zakłóceń w ustroju lub gospodarce RP, innego państwa lub organizacji międzynarodowej,

– a także groźba popełnienia takiego czynu.

Jednak polska definicja, wbrew definicji zawartej w dyrektywie 2017/541, nie określa rodzajów przestępstw bazowych, a jedynie określa je przez wskazanie, że ich górna granica wynosi co najmniej 5 lat. Na marginesie warto zauważyć, że ta odmienność była wskazywana jako brak właściwego wdrożenia dyrektywy[27], z drugiej strony zapewnia jednak elastyczność stosowania krajowej regulacji.

W kontekście stosowania rozporządzenia 2021/784 oraz zabezpieczenia przed ewentualnymi nadużyciami najważniejsza jest właściwa ocena

eliminowaniu danych komputerowych lub czynieniu ich niedostępnymi. Niezgodna z prawem ingerencja w dane to natomiast umyślne i bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi.

[27] Kwestia ta była podnoszona m.in. podczas wizyty w Polsce Dyrekcji Wykonawczej Komitetu Organizacji Narodów Zjednoczonych ds. Zwalczania Terroryzmu (United Nations Counter-Terrorism Committee Executive Directorate, UN CTED), której celem było dokonanie ewaluacji wdrożonych przez Polskę rezolucji Rady Bezpieczeństwa ONZ w zakresie walki z terroryzmem.

faktu ujawnienia treści o charakterze terrorystycznym. Wskazówkę w tym zakresie zawiera motyw 11 tego rozporządzenia. Zgodnie z nim, z uwagi na potrzebę przeciwdziałania najbardziej szkodliwej propagandzie terrorystycznej w internecie, definicja treści o charakterze terrorystycznym powinna obejmować:

> (...) materiały, które podżegają lub nakłaniają kogoś do popełniania przestępstw terrorystycznych lub do przyczynienia się do ich popełniania, materiały, które nakłaniają kogoś do uczestniczenia w działaniach grupy terrorystycznej lub które pochwalają działalność terrorystyczną, w tym poprzez rozpowszechnianie materiałów przedstawiających atak terrorystyczny. Definicja ta powinna także obejmować materiały, które udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji, jak również substancji chemicznych, biologicznych, radiologicznych i jądrowych (CBRJ), lub instruktażu w zakresie innych szczególnych metod lub technik, w tym w zakresie wyboru celów, w celu popełniania przestępstw terrorystycznych lub przyczynienia się do ich popełniania. Materiały takie obejmują tekst, obrazy, nagrania dźwiękowe i nagrania wideo, a także transmisje na żywo przestępstw terrorystycznych, które stwarzają niebezpieczeństwo popełnienia kolejnych takich przestępstw.

Dalsza część tego motywu rozporządzenia 2021/784 wskazuje, że przy ocenie, czy materiały stanowią treści o charakterze terrorystycznym, właściwe organy oraz dostawcy usług hostingowych powinni uwzględniać takie czynniki, jak charakter i treść komunikatów, kontekst, w jakim komunikaty te zostały przedstawione, oraz to, w jakim stopniu mogą one spowodować skutki szkodliwe dla bezpieczeństwa i ochrony osób. W motywie tym sformułowano jednak istotne ograniczenie. Zgodnie z nim ważny czynnik w tej ocenie stanowi fakt, że dany materiał został wyprodukowany przez osobę, grupę lub podmiot umieszczone w unijnym wykazie osób, grup i podmiotów uczestniczących w aktach terrorystycznych i podlegających środkom ograniczającym, że można go przypisać takiej osobie, grupie lub podmiotowi lub że jest on rozpowszechniany w imieniu takiej osoby, grupy lub podmiotu. Z jednej strony ma to służyć zapewnieniu wolności słowa i opinii, z drugiej strony, przy wykładni literalnej, a nie celowościowej, stanowi zawężanie danej treści do powiązania z osobami, grupami lub podmiotami umieszczonymi w unijnym wykazie osób, grup i podmiotów

uczestniczących w aktach terrorystycznych. Nie każdy bowiem dostawca tego rodzaju treści może wprost wykazywać tego rodzaju powiązanie.

W art. 1 ust. 3 rozporządzenia 2021/784 wskazano natomiast wprost, że nie uznaje się za treści o charakterze terrorystycznym materiałów publicznie rozpowszechnianych w celach edukacyjnych, dziennikarskich, artystycznych lub badawczych bądź w celach zapobiegania terroryzmowi lub zwalczania terroryzmu, w tym materiałów służących wyrażaniu polemicznych lub kontrowersyjnych poglądów w ramach debaty publicznej. Co więcej, to w drodze oceny ma być ustalane, jaki jest rzeczywisty cel rozpowszechniania danych treści. Warto w tym kontekście wspomnieć o motywie 12 rozporządzenia 2021/784. Zgodnie z nim przy ustalaniu, czy dany materiał dostarczony przez dostawcę treści stanowi „treści o charakterze terrorystycznym", należy uwzględnić zwłaszcza prawo do wolności wypowiedzi i informacji, w tym wolność i pluralizm mediów, oraz wolność sztuki i nauki.

Z perspektywy legislacyjnej warto zwrócić uwagę na spójność konstrukcyjną terminologii stosowanej w Kodeksie karnym, ustawie o działaniach AT i rozporządzeniu 2021/784. Wskazane akty prawne posługują się odpowiednio terminami „przestępstwo o charakterze terrorystycznym", „zdarzenie o charakterze terrorystycznym" i „treści o charakterze terrorystycznym". Jednak nie wszystkie polskie akty prawne je uwzględniają. Na przykład w ustawie o ABW oraz AW jest mowa o „przestępstwie terroryzmu".

Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784.

Przy analizie zakresu wskazanej właściwości na początku należy zwrócić uwagę na wspomniany wcześniej art. 12 rozporządzenia 2021/784, zgodnie z którym każde państwo członkowskie wyznacza organ lub organy właściwe w zakresie:

- wydawania nakazów zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści terrorystycznych we wszystkich państwach członkowskich (nakaz usunięcia),
- weryfikowania nakazów usunięcia wydanych przez właściwe organy innych państw członkowskich oraz stwierdzania ewentualnych

naruszeń w tym zakresie (procedura dotycząca transgranicznych nakazów usunięcia),
- nadzoru nad wdrażaniem środków szczególnych przez dostawcę usług hostingowych,
- nakładania kar za złamanie przepisów przedmiotowego rozporządzenia.

Powyższe wskazanie nie wyczerpuje wszystkich obowiązków i uprawnień nakładanych na organy właściwe w innych przepisach rozporządzenia 2021/784. W tym zakresie można wskazać m.in. na:
- 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),
- 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,
- 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,
- publikację sprawozdania, na podstawie art. 8 rozporządzenia 2021/784,
- przekazywanie do KE rocznej informacji na podstawie art. 21 rozporządzenia 2021/784.

We wskazanym art. 12 rozporządzenia 2021/784 unijny prawodawca przewidział możliwość wyznaczenia różnych organów jako organów właściwych do realizacji wskazanych uprawnień i obowiązków. Polski ustawodawca nie skorzystał z tej możliwości i wskazał Szefa ABW jako jedyny organ właściwy na gruncie krajowym. Rozwiązanie to wydaje się optymalne i wpisuje się w całokształt krajowych unormowań w tym zakresie, w związku z czym należy zwrócić uwagę na przynajmniej cztery aspekty. Po pierwsze, Szef ABW zgodnie z art. 3 ust. 1 ustawy o działaniach AT odpowiada za zapobieganie zdarzeniom o charakterze terrorystycznym[28]. Po drugie, na podstawie art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW do zadań tej formacji

[28] Zob. szerzej: P. Burczaniuk, *Zadania i uprawnienia organów ścigania karnego w zakresie zwalczania terroryzmu w Polsce – perspektywa prawna*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 9–30. https://doi.org/10.4467/27204383TER.22.017.16337.

należy m.in. rozpoznawanie i wykrywanie przestępstw terroryzmu oraz zapobieganie im, a treści o charakterze terrorystycznym w dużej mierze służą przeprowadzeniu zamachów o charakterze terrorystycznym. Po trzecie, już wcześniej Szef ABW uzyskał kompetencję do blokowania treści o charakterze terrorystycznym na podstawie przepisów ustawy o ABW oraz AW. Po czwarte, ABW ma również strukturę organizacyjną w postaci Centrum Antyterrorystycznego ABW, w pełni przygotowaną do realizacji tego celu, działającą w trybie całodobowym.

Zgodnie z motywem 35 rozporządzenia 2021/784 państwa członkowskie powinny mieć możliwość decydowania o liczbie właściwych organów, które mają zostać wyznaczone, a także o tym, czy mają to być organy administracyjne, organy ścigania czy organy sądowe. Organy te muszą wypełniać swoje zadania w sposób obiektywny i niedyskryminacyjny oraz nie powinny zwracać się o instrukcje do żadnego innego organu w związku z wykonywaniem zadań powierzonych im na podstawie tego rozporządzenia. Co jednak istotne, nie powinno to wykluczać sprawowania nadzoru zgodnie z krajowym prawem konstytucyjnym.

Na podstawie art. 12 ust. 4 rozporządzenia 2021/784 KE utworzyła i na bieżąco aktualizuje internetowy rejestr zawierający wykaz właściwych organów w poszczególnych państwach oraz ich punktów kontaktowych wyznaczonych lub ustanowionych na podstawie art. 12 ust. 2 rozporządzenia, o którym mowa w dalszej części artykułu, w komentarzu do art. 26b ustawy o działaniach AT[29]. Zgodnie z rejestrem opublikowanym na stronie internetowej KE w dniu, gdy polski parlament przyjmował rozwiązania w zakresie blokowania treści, z 27 państw członkowskich UE, takie informacje przekazało 25 (zgłoszeń nie dokonały Słowenia i Portugalia)[30]. Z tej grupy 13 państw wyznaczyło organ właściwy – analogicznie jak Polska – spośród służb o charakterze policyjnym lub specjalnym, cztery państwa wskazały na właściwość komórki organizacyjnej funkcjonującej w ramach ministerstwa spraw wewnętrznych i tyle samo państw w innych urzędach centralnych, np. w przypadku Węgier to Narodowy Urząd ds. Mediów i Komunikacji (Nemzeti Média- és Hírközlési Hatóság), w Austrii – Urząd do

[29] *List of national competent authority (authorities) and contact points*, European Commission, 27 I 2025 r., 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?prefLang=pl [dostęp: 15 II 2025].

[30] Na 23 II 2025 r. jedynym państwem, które nie dokonało zgłoszenia, była Portugalia.

Spraw Łączności (Kommunikationsbehörde Austria). W dwóch państwach jest to organ prokuratorski, a w jednym właściwy jest sąd[31].

Decyzja polskiego ustawodawcy, tj. wskazanie Szefa ABW jako organu właściwego, jest zgodna z wytycznymi UE i nie odbiega od rozwiązań przyjętych w innych państwach, jednak praktyka w tym zakresie jest różna.

> Art. 26b. 1. Szef ABW wyznacza w ABW punkt kontaktowy, o którym mowa w art. 12 ust. 2 rozporządzenia 2021/784, działający w systemie całodobowym przez 7 dni w tygodniu.
> 2. Informacje o siedzibie i danych kontaktowych punktu, o którym mowa w ust. 1, oraz sposobie składania wniosków o wyjaśnienie i informacje zwrotne w sprawie nakazów usunięcia zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści o charakterze terrorystycznym, zwanych dalej „nakazami usunięcia", udostępnia się w Biuletynie Informacji Publicznej na stronie podmiotowej ABW.

Artykułem 12 ust. 2 rozporządzenia 2021/784 państwa członkowskie zostały zobowiązane do zapewnienia, że w ramach organu właściwego do wydawania nakazów usunięcia zostanie wyznaczony lub ustanowiony punkt kontaktowy zajmujący się wnioskami o wyjaśnienie i informacjami zwrotnymi, które dotyczą tych nakazów. W Polsce konsekwencją wyboru Szefa ABW jako organu właściwego było wyznaczenie przez niego punktu kontaktowego w kierowanej przez siebie Agencji. Państwa członkowskie zostały również zobowiązane do zapewnienia, że informacje na temat punktu kontaktowego będą publicznie dostępne.

Warto zauważyć, że polski ustawodawca rozszerzył minimalny zakres informacji zamieszczonych na stronie podmiotowej stosownie do wymogów wynikających z rozporządzenia 2021/784. Oprócz informacji o punkcie kontaktowym na stronie podmiotowej musi się znajdować również informacja o sposobie składania wniosków o wyjaśnienie i informacje zwrotne w sprawie nakazów usunięcia. Zgodnie z komunikatem zawartym na stronie ABW:

> Wnioski o wyjaśnienie w sprawie nakazów usunięcia zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści o charakterze

[31] Zob. szerzej: *Rządowy projekt ustawy o zmianie ustawy…*

terrorystycznym, złożone przy użyciu wzoru określonego w załączniku nr III do rozporządzenia 2021/784, można kierować w postaci papierowej na adres pocztowy punktu kontaktowego bądź w postaci elektronicznej na adres e-mail punktu kontaktowego. Informacje zwrotne po usunięciu treści o charakterze terrorystycznym lub uniemożliwieniu dostępu do nich, złożone przy użyciu wzoru określonego w załączniku nr II do rozporządzenia 2021/784, będą przekazywane w tej samej postaci[32].

Należy odnotować, że punkt kontaktowy jest przeznaczony wyłącznie dla dostawców usług hostingowych, których dotyczy nakaz usunięcia. Agencja Bezpieczeństwa Wewnętrznego nie prowadzi ogólnego portalu zgłaszania nielegalnych treści w internecie.

Art. 26c. 1. Szef ABW sprawuje nadzór nad wdrażaniem środków szczególnych, o których mowa w art. 5 ust. 1–3 rozporządzenia 2021/784, przez:
1) dokonywanie kontroli środków szczególnych, które podjął dostawca usług hostingowych, w tym pod kątem ich zgodności z art. 5 ust. 2 i 3 rozporządzenia 2021/784;
2) wydawanie dostawcy usług hostingowych pisemnych zaleceń, mających na celu usunięcie stwierdzonych nieprawidłowości i dostosowanie jego działalności do przepisów rozporządzenia 2021/784.

2. Upoważniony funkcjonariusz ABW, przeprowadzając czynności, o których mowa w ust. 1, ma prawo:
1) wstępu na teren kontrolowanych obiektów wykorzystywanych do świadczenia usług hostingowych;
2) żądania od dostawcy usług hostingowych wyjaśnień i udostępnienia dokumentacji technicznej i operacyjnej wynikającej ze stosowania środków szczególnych bądź wglądu w tę dokumentację.

3. Dostawca usług hostingowych narażony na treści o charakterze terrorystycznym usuwa naruszenia przepisów prawa i nieprawidłowości stwierdzone w ramach nadzoru sprawowanego przez Szefa ABW w terminie określonym w pisemnym zaleceniu.

Umożliwienie objęcia dostawcy usług hostingowych środkami szczególnymi przez uznanie go za dostawcę narażonego na treści o charakterze terrorystycznym jest powiązane z zobowiązaniem państw do zapewnienia przez właściwe organy skutecznych funkcji nadzorczych. Jak wskazano

[32] *Punkt kontaktowy TCO*, BIP ABW, https://bip.abw.gov.pl/bip/punkt-kontatowy-tco/525, Punkt-kontaktowy-TCO.html [dostęp: 13 XII 2024].

wcześniej, wdrażane przez dostawcę usług hostingowych środki zabezpieczające mogą dotyczyć odpowiednich środków technicznych i operacyjnych umożliwiających użytkownikom zgłaszanie treści o charakterze terrorystycznym, a także innych mechanizmów zwiększających świadomość odbiorców treści. Jeżeli natomiast właściwy organ uzna, że podjęte środki szczególne nie są zgodne z wymogami, kieruje on do dostawcy usług hostingowych decyzję zobowiązującą go do podjęcia niezbędnych środków uzupełniających lub naprawczych.

Zapewnienie stosowania tych przepisów wymagało wskazania, że Szef ABW sprawuje nadzór nad wdrażaniem środków szczególnych, który będzie polegał ma dokonywaniu kontroli środków szczególnych stosowanych przez dostawcę usług hostingowych, a także na wydawaniu mu pisemnych zaleceń w przypadku stwierdzenia nieprawidłowości w tym zakresie.

W celu zapewnienia wykonania tych czynności upoważniony funkcjonariusz ABW ma prawo wstępu na teren kontrolowanych obiektów wykorzystywanych do świadczenia usług hostingowych oraz żądania od dostawcy usług hostingowych wyjaśnień i udostępnienia dokumentacji technicznej i operacyjnej wynikającej ze stosowania środków szczególnych bądź wglądu w nią.

W myśl przepisów dostawca usług hostingowych jest zobowiązany do terminowego usunięcia stwierdzonych nieprawidłowości.

Wprowadzone przepisy z jednej strony w niektórych elementach nawiązują do *Ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia*, z drugiej zaś, co niezwykle istotne z perspektywy zasad realizacji czynności, nie wyłączają stosowania ustawy – Prawo przedsiębiorców.

W kontekście ustawy o ochronie osób i mienia warto zwrócić uwagę na brzmienie jej art. 43 ust. 2 pkt 3–5, który określa zasady nadzoru Komendanta Głównego Policji nad działalnością specjalistycznych uzbrojonych formacji ochronnych. Wskazany tam nadzór polega m.in. na wstępie na teren siedziby przedsiębiorcy prowadzącego działalność i wydawaniu pisemnych zaleceń mających na celu usunięcie stwierdzonych nieprawidłowości i dostosowanie działalności tych formacji do przepisów prawa.

W uzasadnieniu do rządowego projektu ustawy o zmianie ustawy o działaniach AT i ustawy o ABW oraz AW stwierdzono natomiast: *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[33].

W kontekście art. 48 ustawy – Prawo przedsiębiorców należy zwrócić uwagę m.in. na obowiązek zawiadamiania przedsiębiorcy przez organ kontroli o zamiarze wszczęcia kontroli. Wszczyna się ją nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia zawiadomienia o zamiarze wszczęcia kontroli. Na wniosek przedsiębiorcy może być ona wszczęta przed upływem 7 dni od dnia doręczenia zawiadomienia. Z czynności kontrolnych wykonywanych w trybie związanych z oględzinami sporządza się protokół.

Zgodnie z art. 49 tej regulacji czynności kontrolne mogą być wykonywane przez pracowników organu kontroli po okazaniu przedsiębiorcy albo osobie przez niego upoważnionej legitymacji służbowej upoważniającej do wykonywania takich czynności oraz po doręczeniu upoważnienia do przeprowadzenia kontroli. Jej zakres nie może wykraczać poza ten wskazany w upoważnieniu.

Na podstawie art. 51–57 tej ustawy kontrolę przeprowadza się, co do zasady, w siedzibie przedsiębiorcy lub w miejscu wykonywania działalności gospodarczej oraz w godzinach pracy lub w czasie faktycznego wykonywania działalności gospodarczej przez przedsiębiorcę. Czynności kontrolne wykonuje się jak najsprawniej i tak, by w miarę możliwości nie zakłócić funkcjonowania przedsiębiorcy. Ustalenia kontroli zamieszcza się w protokole. W przypadku gdy przedsiębiorca wskaże na piśmie, że wykonywane czynności zakłócają w sposób istotny działalność gospodarczą przedsiębiorcy, konieczność podjęcia takich czynności uzasadnia się w protokole kontroli. Ponadto ma zastosowanie zakaz podejmowania i prowadzenia więcej niż jednej kontroli działalności przedsiębiorcy. Czas trwania wszystkich kontroli u przedsiębiorcy w jednym roku kalendarzowym zależy od wielkości przedsiębiorstwa. Przedłużenie czasu trwania kontroli jest możliwe jedynie z przyczyn niezależnych od organu kontroli i wymaga uzasadnienia na piśmie.

Wskazane normy wynikające z ustawy – Prawo przedsiębiorców nie wyczerpują całości uregulowań w zakresie kontroli, jednak na podstawie przywołanych rozwiązań należy podkreślić, że kontrola stosowania środków szczególnych jest prowadzona na standardowych zasadach przewidzianych dla kontroli przedsiębiorców i nie zawiera wyróżniających się rozwiązań.

[33] *Rządowy projekt ustawy o zmianie ustawy...* – uzasadnienie..., s. 9.

Art. 26d. 1. Nakaz usunięcia lub stwierdzenie naruszenia, o którym mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/784, następuje w drodze decyzji administracyjnej. Do postępowań w tych sprawach w zakresie nieuregulowanym w rozporządzeniu 2021/784 i niniejszej ustawie stosuje się przepisy art. 6, art. 7, art. 7b, art. 8, art. 12, art. 14, art. 16, art. 24, art. 26 § 1 i 2, art. 28–30, art. 32, art. 33, art. 35 § 1, art. 50, art. 54–56, art. 63–65, art. 72, art. 75 § 1, art. 77, art. 97 § 1 pkt 4 i § 2, art. 104, art. 105 § 1, art. 112, art. 113 § 1, art. 156–158, art. 217 oraz art. 268a ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2024 r. poz. 572).

2. Wskazywanie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, o których mowa w art. 5 rozporządzenia 2021/784, następuje w drodze decyzji administracyjnej. Do postępowań w tych sprawach stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, o których mowa w ust. 1, oraz art. 107 tej ustawy.
3. Decyzje, o których mowa w ust. 1 i 2, są ostateczne i podlegają natychmiastowemu wykonaniu.
4. Dostawcy usług hostingowych, w stosunku do którego Szef ABW wydał nakaz usunięcia, lub dostawcy treści, którego treści obejmuje nakaz usunięcia, przysługuje prawo do wniesienia na ten nakaz skargi do sądu administracyjnego w terminie 30 dni od dnia:
   1) jego dostarczenia w trybie, o którym mowa w art. 3 ust. 5 rozporządzenia 2021/784 – w przypadku dostawcy usług hostingowych;
   2) otrzymania informacji, o której mowa w art. 11 ust. 1 rozporządzenia 2021/784 – w przypadku dostawcy treści.
5. Dostawcy usług hostingowych lub dostawcy treści, w stosunku do którego Szef ABW wydał decyzję, o której mowa w art. 4 ust. 4 rozporządzenia 2021/784, przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego w terminie 30 dni od dnia otrzymania powiadomienia o tej decyzji.
6. Dostawcy usług hostingowych, w stosunku do którego Szef ABW wydał decyzję, o której mowa w art. 5 ust. 4, 6 lub 7 rozporządzenia 2021/784, przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego.
7. Skargi, o których mowa w ust. 4–6, mogą być rozpoznawane w trybie uproszczonym, o którym mowa w art. 120 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2024 r. poz. 935), o ile strona nie zawnioskuje o przeprowadzenie rozprawy, a sąd uzna, że wszystkie okoliczności sprawy zostały dostatecznie wyjaśnione i przeprowadzenie rozprawy jest zbędne. Przepis art. 122 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi stosuje się.

W świetle brzmienia art. 26d ust. 1 i 2 nakaz usunięcia lub stwierdzenie naruszenia w procedurze dotyczącej transgranicznych nakazów usunięcia, a także wskazywanie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym następują w drodze decyzji administracyjnej. Norm proceduralnych do wydawania decyzji dostarcza zatem nie tylko rozporządzenie 2021/784 czy znowelizowana ustawa o działaniach AT, lecz także *Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego* (dalej: k.p.a.). Zakres stosowania k.p.a. jest jednak znacznie ograniczony przez enumeratywne wskazanie konkretnych przepisów.

To, czy rzeczywiście tak głębokie wyłączenie k.p.a. pozwala realnie traktować nakaz usunięcia jako decyzję administracyjną, może być dyskusyjne, szczególnie w kontekście braku zastosowania w tych sprawach art. 107 k.p.a. określającego niezbędne elementy decyzji. Jednak jak wskazano w uzasadnieniu do ustawy:

> 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[34].

W uzasadnieniu do ustawy wskazano również, że przyjęty w art. 26d ust. 1 katalog przepisów k.p.a. jest wzorowany na 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*

[34] *Rządowy projekt ustawy o zmianie ustawy...* – uzasadnienie..., s. 9–10.

narodowego[35]. Dokonano jednak niezbędnych uzupełnień i dostosowania do mechanizmu postępowania wynikającego wprost z przepisów rozporządzenia 2021/784.

Należy zatem zauważyć, że do postępowań prowadzonych w sprawach nakazów oraz wskazania dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym (środki szczególne) mają zastosowanie podstawowe zasady k.p.a., w tym:

- zasada praworządności (art. 6),
- zasada prawdy obiektywnej (art. 7),
- zasada uwzględniania interesu społecznego i słusznego interesu obywateli (art. 7),
- zasada zaufania do władzy publicznej (art. 8),
- zasada szybkości i prostoty postępowania (art. 12),
- zasada pisemności postępowania (art. 14),
- zasada trwałości decyzji administracyjnych (art. 16).

Powyższe przepisy mają charakter ściśle gwarancyjny z perspektywy ochrony interesów strony. Obiektywność postępowań jest zabezpieczona również przez możliwość wyłączenia pracownika danego organu od udziału w postępowaniu, zgodnie z art. 24 k.p.a.

Z perspektywy stron warto także wspomnieć o stosowaniu art. 28 i 29 k.p.a., zgodnie z którymi stroną jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie, albo kto żąda czynności organu ze względu na swój interes prawny lub obowiązek. Stronami mogą być osoby fizyczne i osoby prawne, a gdy chodzi o państwowe i samorządowe jednostki organizacyjne i organizacje społeczne – również jednostki nieposiadające osobowości prawnej.

W przeciwieństwie do wspomnianego wzorca z ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, w sprawach objętych analizowaną regulacją ma zastosowanie cały art. 77 k.p.a. Zgodnie z nim organ jest zobowiązany w sposób wyczerpujący zebrać i rozpatrzyć cały materiał dowodowy, może też w każdym stadium postępowania zmienić, uzupełnić lub uchylić swoje postanowienie dotyczące przeprowadzenia dowodu. Organ przeprowadzający postępowanie na wezwanie organu

[35] Zob. szerzej: M. Cichomski, *Między konfliktem zbrojnym a terroryzmem państwowym – szczególne indywidualne środki ograniczające przyjęte w Polsce w kontekście wojny w Ukrainie i sytuacji w Białorusi. Perspektywa prawna*, „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 118–121. https://doi.org/10.4467/27204383TER.24.003.19391.

właściwego do załatwienia sprawy (art. 52 k.p.a.) może też z urzędu lub na wniosek strony przesłuchać nowych świadków i biegłych na okoliczności będące przedmiotem tego postępowania.

Analogicznie do nakazów usunięcia oraz stwierdzania naruszeń w formie decyzji administracyjnej następuje także wskazanie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, zgodnie z art. 5 rozporządzenia 2021/784. Do tych decyzji k.p.a. również ma zastosowanie, lecz w ograniczonym zakresie. W tym wypadku jednak, w przeciwieństwie do postępowań związanych z wydaniem nakazu usunięcia lub stwierdzenia naruszenia, o którym mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/748, ma zastosowanie art. 107 k.p.a., czyli przepis określający elementy decyzji. Wynika to z faktu, że ww. rozporządzenie w tym wypadku nie określa formy ani elementów składowych tego rozstrzygnięcia.

Jednocześnie we wszystkich tych przypadkach postępowania są jednoinstancyjne, a wydane decyzje podlegają natychmiastowej wykonalności, co wiąże się z potrzebą zapewnienia sprawności i efektywności prowadzenia takich postępowań. W kontekście jednoinstancyjności postępowań administracyjnych należy przywołać art. 78 Konstytucji RP, zgodnie z którym każda ze stron ma prawo do zaskarżenia orzeczeń i decyzji wydanych w pierwszej instancji, a wyjątki od tej zasady oraz tryb zaskarżania określa ustawa. Konstytucja RP dopuszcza zatem takie rozwiązanie, ale stanowi ono odstępstwo od zasady, co musi mieć swoje uzasadnienie. W tej sytuacji należy go szukać w konstytucyjnej przesłance zapewnienia bezpieczeństwa i porządku publicznego. Zgodnie bowiem z art. 31 ust. 3 Konstytucji RP ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw, w tym wypadku prawa zaskarżenia decyzji wydanej w pierwszej instancji, mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w państwie demokratycznym dla jego bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw. W tym wypadku brak możliwości zaskarżenia decyzji pierwszej instancji nie wydaje się, w opinii autora, naruszać istoty praw, o których mowa powyżej, pozostaje bowiem droga sądowa. Osobna kwestia to natomiast ocena, czy to rozwiązanie jest konieczne w państwie demokratycznym dla jego bezpieczeństwa lub porządku publicznego. Ono również wydaje się spełniać ten wymóg konstytucyjny. Wprawdzie można sobie wyobrazić, że wskutek zaskarżenia decyzji Szef ABW będzie rozpatrywał wniosek o ponowne rozpatrzenie sprawy, jednak istota

rozstrzyganych spraw wymaga natychmiastowej wykonalności. Nakaz usunięcia nie może oczekiwać na uprawomocnienie, bo jego istotą jest natychmiastowe uniemożliwienie rozpowszechniania treści o charakterze terrorystycznym. Okres oczekiwania na uprawomocnienie decyzji pozbawiłby to narzędzie prawne znaczenia zapobiegawczego, ponieważ nakaz usunięcia to nie kara, lecz instrument prewencyjny. Dopiero na podstawie innych przepisów prawnych w oddzielnym postępowaniu, już nie administracyjnym, lecz karnym, jest możliwe ukaranie dostawcy takiej treści. Analogicznie należałoby postrzegać rozwiązanie, zgodnie z którym zaskarżenie decyzji następowałoby do organu drugiej instancji, czyli organu nadzorującego formację, w tym wypadku Prezesa Rady Ministrów.

Dostawcy usług hostingowych, w stosunku do którego Szef ABW wydał nakaz usunięcia, lub dostawcy treści, którego treści obejmuje nakaz usunięcia, przysługuje prawo do wniesienia skargi do sądu administracyjnego w terminie 30 dni. W pierwszym przypadku termin ten jest liczony od dostarczenia decyzji, a w drugim przypadku – od dnia otrzymania informacji. W tym zakresie art. 26d ustawy jest wykonaniem art. 9 rozporządzenia 2021/784, który przyznaje prawo do zaskarżania wydanych nakazów usunięcia oraz pozostałych decyzji wydanych przez organ właściwy.

W przypadku dostawcy usług hostingowych właściwy organ kieruje nakaz usunięcia do jego głównej jednostki organizacyjnej lub do jego przedstawiciela prawnego. Nakaz usunięcia jest przekazywany punktowi kontaktowemu dostawcy usług hostingowych za pomocą środków elektronicznych dających możliwość sporządzenia pisemnego potwierdzenia na warunkach umożliwiających ustalenie autentyczności nadawcy, w tym podanie dokładnej daty oraz godziny wysłania i otrzymania nakazu.

Dostawcy usług hostingowych lub dostawcy treści, w stosunku do którego Szef ABW wydał decyzję we wspomnianej procedurze dotyczącej transgranicznych nakazów usunięcia, przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego w terminie 30 dni od dnia otrzymania powiadomienia o tej decyzji.

Również dostawcy usług hostingowych, który został uznany za dostawcę szczególnie narażonego na treści o charakterze terrorystycznym (środki szczególne), przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego.

Skargi wniesione we wszystkich z ww. przypadków mogą być rozpoznawane w trybie uproszczonym, o którym mowa w art. 120 *Ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi,*

tj. na posiedzeniu niejawnym w składzie trzech sędziów, o ile strona nie zawnioskuje o przeprowadzenie rozprawy, a sąd uzna, że wszystkie okoliczności sprawy zostały dostatecznie wyjaśnione i przeprowadzenie rozprawy jest zbędne. Jak wskazano w uzasadnieniu do ustawy, to rozwiązanie ma zapewnić, że rozpatrywanie środków sądowego zaskarżenia decyzji będzie realizowane sprawnie i efektywnie, z zachowaniem wszelkich gwarancji prawa do sądu[36].

Przyjęta w ustawie procedura jest procedurą administracyjną. Zgodnie z uzasadnieniem do projektu:

> 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 [niego] 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[37].

W toku prac parlamentarnych nad ustawą było rozpatrywane jeszcze jedno rozwiązanie, które miało usprawnić etap prowadzonego postępowania sądowego. Zgodnie z nim przekazanie akt i odpowiedzi na skargę do sądu administracyjnego następowałaby w terminie 15 dni od dnia otrzymania skargi, skarga zaś byłaby rozpatrywana przez Wojewódzki Sąd Administracyjny (WSA) w terminie 30 dni od dnia otrzymania akt i odpowiedzi na skargę[38]. To rozwiązanie było wzorowane na art. 21 *Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej*. Strona rządowa, czyli projektodawca, negatywnie odniosła się do propozycji. Wskazała, że nie zagwarantuje ona rzeczywistego przyspieszenia rozpatrywania

[36] *Rządowy projekt ustawy o zmianie ustawy*... – uzasadnienie..., s. 11.

[37] Tamże.

[38] *Sprawozdanie Komisji Administracji i Spraw Wewnętrznych oraz Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii o rządowym projekcie ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (druk nr 661)*, druk nr 706, https://orka.sejm.gov.pl/Druki10ka.nsf/0/C75A45601BC82E4EC1258BB3003DFB3A/%24File/706.pdf [dostęp: 21 XII 2024].

ewentualnych skarg na etapie sądowym, ponieważ zawarte w niej terminy w odniesieniu do sądu mają charakter instrukcyjny.

Strona rządowa zaproponowała inne rozwiązanie – rozważenie przez Prezydenta RP zastosowania art. 13 § 3 ustawy – Prawo o postępowaniu przed sądami administracyjnymi przez wydanie rozporządzenia, na którego podstawie nie tylko WSA w Warszawie, lecz także inne wojewódzkie sądy administracyjne, np. właściwe według miejsca zamieszkania lub siedziby skarżącego albo miejsca pobytu lub siedziby jego przedstawiciela prawnego, mogłyby rozpoznawać sprawy z zakresu skarg na decyzje wydane przez Szefa ABW. Alternatywnym rozwiązaniem mogłoby być również wskazanie na stałe właściwości WSA innego niż ten w Warszawie.

> Art. 26e. Dostawca usług hostingowych, w stosunku do którego został wydany nakaz usunięcia, w terminie do dnia 1 marca każdego roku przekazuje Szefowi ABW dane, o których mowa w art. 21 ust. 1 lit. b i d rozporządzenia 2021/784, za rok poprzedni.

Przywołany art. 21 ust. 1 rozporządzenia 2021/784 zobowiązuje państwa członkowskie do gromadzenia i przekazywania do KE, do 31 marca każdego roku, informacji, które uzyskały od swoich właściwych organów i dostawców usług hostingowych podlegających ich jurysdykcji za poprzedni rok kalendarzowy. Informacje te, zgodnie z rozporządzeniem 2021/784, obejmują:

- liczbę wydanych nakazów usunięcia oraz liczbę przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, a także szybkość, z jaką dokonano usunięcia lub uniemożliwiono dostęp;
- środki szczególne podjęte na podstawie rozporządzenia, w tym liczbę przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, a także szybkość, z jaką dokonano usunięcia lub uniemożliwiono dostępu;
- liczbę wniosków o dostęp, z którymi wystąpiły właściwe organy, w odniesieniu do treści zachowywanych przez dostawcę usług hostingowych na podstawie art. 6 rozporządzenia (dostawcy usług hostingowych zachowują treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony w wyniku nakazu usunięcia lub środków szczególnych, które zostały usunięte w wyniku usunięcia takich treści o charakterze

terrorystycznym, które to treści i dane są konieczne do: kontroli w postępowaniach administracyjnych lub sądowych lub rozpatrywania skarg na w przypadku decyzji o usunięciu treści o charakterze terrorystycznym i związanych z nimi danych lub o uniemożliwieniu do nich dostępu; lub zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania);
– liczbę wszczętych procedur rozpatrywania skarg oraz działań podjętych przez dostawców usług hostingowych;
– liczbę wszczętych kontroli w postępowaniach administracyjnych lub sądowych oraz decyzji podjętych przez właściwy organ zgodnie z prawem krajowym.

Art. 26f. 1. Dostawca usług hostingowych, który nie dopełnia obowiązku, o którym mowa w art. 3 ust. 3 lub 6, art. 4 ust. 2 lub 7, art. 5 ust. 1–3, 5 lub 6, art. 6, art. 7, art. 10, art. 11, art. 14 ust. 5, art. 15 ust. 1 lub art. 17 rozporządzenia 2021/784, podlega karze pieniężnej.
2. Karę pieniężną, o której mowa w ust. 1, nakłada Szef ABW, w drodze decyzji administracyjnej, biorąc pod uwagę warunki i okoliczności określone w art. 18 rozporządzenia 2021/784 w wysokości do 4% całkowitych obrotów uzyskanych przez dostawcę usług hostingowych w poprzednim roku obrotowym.
3. Decyzja, o której mowa w ust. 2, jest ostateczna.
4. Środki z kar pieniężnych, o których mowa w ust. 1, stanowią dochód budżetu państwa.

Art. 26f zawiera normy penalizujące w postaci administracyjnych kar pieniężnych za konkretne zachowania stanowiące naruszenie obowiązków określonych w rozporządzeniu 2021/784. Zgodnie z art. 18 rozporządzenia państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń tego aktu prawnego przez dostawców usług hostingowych i podejmują wszelkie środki niezbędne do zapewnienia ich wykonania. Wyliczenie artykułów rozporządzenia 2021/784, w których mowa o obowiązkach dostawcy usług hostingowych, zostało powielone za unijnym prawodawcą w opisywanym art. 26f ustawy. Sankcja może być zastosowana względem dostawcy usług hostingowych w przypadkach, gdy:
– dostawca usług hostingowych nie usunął treści o charakterze terrorystycznym lub nie uniemożliwił dostępu do tych treści we wszystkich państwach członkowskich jak najszybciej, a w każdym razie

zrobił to później niż w ciągu jednej godziny od otrzymania nakazu usunięcia (art. 3 ust. 3);
- dostawca usług hostingowych nie poinformował właściwego organu, przy użyciu wzoru określonego w załączniku II rozporządzenia, o usunięciu treści o charakterze terrorystycznym lub o uniemożliwieniu dostępu do treści terrorystycznych we wszystkich państwach członkowskich, ze wskazaniem w szczególności czasu tego usunięcia lub uniemożliwienia dostępu (art. 3 ust. 6);
- dostawca usług hostingowych, który otrzymał nakaz usunięcia treści o charakterze terrorystycznym w procedurze transgranicznych nakazów usunięcia, nie podjął środków przewidzianych dla nakazów usunięcia lub nie podjął środków niezbędnych, by móc przywrócić usunięte treści lub dostęp do nich (art. 4 ust. 2);
- gdy właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, wydał decyzję o stwierdzeniu naruszenia przepisów rozporządzenia przez organ innego państwa, który wydał nakaz usunięcia, dostawca usług hostingowych natychmiast nie przywrócił danych treści lub dostępu do nich (art. 4 ust. 7);
- dostawca usług hostingowych narażony na treści o charakterze terrorystycznym nie zamieścił w swoich warunkach umownych oraz nie stosuje postanowień mających przeciwdziałać wykorzystywaniu jego usług do publicznego rozpowszechniania treści o charakterze terrorystycznym. Nie działa on przy tym z zachowaniem należytej staranności, w sposób proporcjonalny i niedyskryminacyjny, z uwzględnieniem odpowiednio we wszystkich okolicznościach praw podstawowych użytkowników, zwłaszcza wolności wypowiedzi i informacji w otwartym i demokratycznym społeczeństwie, tak aby uniknąć usuwania materiałów, które nie stanowią treści o charakterze terrorystycznym (art. 5 ust. 1);
- dostawca usług hostingowych narażony na treści o charakterze terrorystycznym nie podejmuje środków szczególnych w celu ochrony swoich usług przed publicznym rozpowszechnianiem treści o charakterze terrorystycznym (art. 5 ust. 2);
- środki szczególne stosowane przez dostawcę usług hostingowych narażonego na treści o charakterze terrorystycznym nie spełniają wszystkich następujących wymogów:

  - skutecznie zmniejszają poziom narażenia usług dostawcy usług hostingowych na treści o charakterze terrorystycznym;
  - są ukierunkowane i proporcjonalne, przy uwzględnieniu poziomu narażenia usług na treści o charakterze terrorystycznym;
  - są stosowane w sposób, który uwzględnia pełne poszanowanie praw i uzasadnionego interesu użytkowników, zwłaszcza podstawowych praw użytkowników dotyczących wolności wypowiedzi i informacji, poszanowania życia prywatnego i ochrony danych osobowych;
  - są stosowane w staranny i niedyskryminacyjny sposób;
- dostawca usług hostingowych narażony na treści o charakterze terrorystycznym nie powiadamia właściwego organu o środkach szczególnych, które podjął i które zamierza podjąć w celu wykonania ciążących na nim obowiązków (art. 5 ust. 5);
- dostawca usług hostingowych narażony na treści o charakterze terrorystycznym nie wykonał decyzji organu właściwego zobowiązującego go do podjęcia dodatkowych niezbędnych środków zabezpieczających (art. 5 ust. 6);
- dostawca usług hostingowych nie zachował treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony w wyniku nakazu usunięcia lub środków szczególnych na podstawie art. 3 lub 5 rozporządzenia, jak również związanych z nimi danych, które to treści i dane są konieczne do kontroli w postępowaniach administracyjnych lub sądowych lub rozpatrywania skarg lub też do zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (art. 6 rozporządzenia);
- dostawca usług hostingowych nie określił w swoich warunkach umownych w sposób jasny swoich zasad dotyczących przeciwdziałania rozpowszechnianiu treści o charakterze terrorystycznym (art. 7);
- dostawca usług hostingowych, który w danym roku kalendarzowym podjął działania mające na celu przeciwdziałanie rozpowszechnianiu treści o charakterze terrorystycznym lub został zobowiązany do podjęcia działań na podstawie niniejszego rozporządzenia, nie udostępnia publicznie ogólnie dostępnego sprawozdania z przejrzystości na temat tych działań za dany rok. Nie publikuje on sprawozdania przed 1 marca kolejnego roku lub sprawozdanie nie zawiera elementów przewidzianych rozporządzeniem (art. 7);

- dostawca usług hostingowych nie ustanowił skutecznego i dostępnego mechanizmu umożliwiającego dostawcom treści, w przypadku gdy ich treści zostały usunięte lub dostęp do nich został uniemożliwiony w wyniku środków szczególnych, złożenia skargi dotyczącej danego usunięcia lub uniemożliwienia dostępu z żądaniem przywrócenia treści lub dostępu do nich (art. 10);
- dostawca usług hostingowych nie rozpatruje skarg i nie przywraca w terminie treści lub dostępu do nich, w przypadku gdy ich usunięcie lub uniemożliwienie dostępu do nich było nieuzasadnione (art. 10);
- dostawca usług hostingowych, który usunął treści o charakterze terrorystycznym lub uniemożliwił dostęp do nich, nie udostępnił dostawcy treści informacji na temat takiego usunięcia lub uniemożliwienia dostępu lub też, mimo wniosku dostawcy treści, nie poinformował go o powodach usunięcia lub uniemożliwienia dostępu oraz o jego prawach do zaskarżenia nakazu usunięcia albo nie udostępniał dostawcy treści kopię nakazu usunięcia (art. 11);
- dostawca usług hostingowych, który dowiedział się o treściach o charakterze terrorystycznym wiążących się z bezpośrednim zagrożeniem życia, nie poinformował natychmiast organu właściwego w zakresie prowadzenia postępowań przygotowawczych i ścigania przestępstw w zainteresowanym państwie członkowskim lub zainteresowanych państwach członkowskich (art. 14 ust. 5);
- dostawca usług hostingowych nie wskazał lub nie ustanowił punktu kontaktowego do celów odbioru nakazów usunięcia za pomocą środków elektronicznych lub nie zapewnił, aby informacje o punkcie kontaktowym były publicznie dostępne (art. 15 ust. 1);
- dostawca usług hostingowych, który nie ma głównej jednostki organizacyjnej w UE, nie wyznaczył osoby fizycznej lub prawnej jako swojego przedstawiciela prawnego w UE do celów odbioru, stosowania się do i wykonywania nakazów usunięcia i decyzji wydanych przez właściwe organy (art. 17).

Wskazane działania lub zaniechania mimo swej dużej liczby nie wyczerpują całości zachowań, które mogą być sankcjonowane na podstawie przepisów katalogowych określonych w art. 26f ust. 1 ustawy. Należy jednak podkreślić ich wielowymiarowość i to, że nie odnoszą się one wyłącznie do kwestii stosowania samych nakazów usunięcia lub środków

szczególnych, lecz dotyczą m.in. realizacji obowiązków związanych z zapewnieniem przejrzystości działań ze strony tych dostawców.

Procedurę nakładania kary i jej formę (przez Szefa ABW w drodze decyzji administracyjnej), a także dyrektywy wymiaru kary i jej maksymalną wysokość ustawodawca określił w art. 26f ust. 2. Zgodnie z przywołanym w tym przepisie art. 18 rozporządzenia 2021/784 Szef ABW przy podejmowaniu decyzji w sprawie nałożenia kary i ustalaniu jej rodzaju i wysokości jest zobowiązany do uwzględnienia wszystkich istotnych okoliczności sprawy, w tym:

- charakteru, wagi i czasu trwania naruszenia;
- umyślności lub charakteru naruszenia wynikającego z zaniedbania;
- wcześniejszego naruszenia popełnionego przez dostawcę usług hostingowych;
- kondycji finansowej dostawcy usług hostingowych;
- poziomu współpracy dostawcy usług hostingowych z właściwymi organami;
- charakteru i rozmiaru dostawców usług hostingowych, zwłaszcza tego, czy jest on mikro-, małym lub średnim przedsiębiorstwem;
- stopnia winy dostawcy usług hostingowych, z uwzględnieniem podjętych przez niego środków technicznych i organizacyjnych w celu spełnienia wymogów rozporządzenia.

Przyjęta w przepisie maksymalna kara administracyjna, która może być orzeczona na podstawie przepisów ustawy, również wynika wprost z rozporządzenia 2021/784. W jego art. 18 ust. 3 jest wskazane, że państwa członkowskie zapewniają, że systematyczne lub uporczywe niedopełnianie obowiązków będzie podlegało karom pieniężnym w wysokości do 4% całkowitych obrotów dostawcy usług hostingowych w poprzednim roku obrotowym.

Należy ponadto zauważyć, że ustawa, w zakresie prowadzonych postępowań, nie wyłącza ani nie ogranicza stosowania k.p.a. W efekcie Szef ABW będzie miał możliwość skorzystania z narzędzi łagodzących karę, np. z instytucji jej odroczenia albo rozłożenia na raty. Zasada proporcjonalności jest 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 (art. 189f k.p.a.)[39].

[39] *Rządowy projekt ustawy o zmianie ustawy...* – uzasadnienie..., s. 13.

Decyzje Szefa ABW mają charakter ostateczny, dlatego również w tym przypadku zostały wyłączone pozasądowe mechanizmy zaskarżenia.

Środki z kar pieniężnych stanowią dochód budżetu państwa. W tym kontekście warto przywołać ocenę skutków regulacji, załączoną do projektu ustawy, zgodnie z którą (...) *projektowana ustawa przewiduje nakładanie przez Szefa ABW na dostawców usług hostingowych administracyjnych kar pieniężnych za naruszenia wynikające z rozporządzenia, które będą stanowiły dochód budżetu państwa, należy z tego tytułu prognozować przychód do budżetu państwa. Niemniej trzeba przyjąć, że będzie on znikomy, a ponadto niemożliwy na tym etapie do zwymiarowania*[40]. Zapis ten wskazuje, że w opinii projektodawcy rzeczywiste zastosowanie rozporządzenia 2021/784 i samej ustawy będzie incydentalne, a poziom zagrożenia w Polsce rozpowszechnianiem treści o charakterze terrorystycznym jest niski. Ta opinia wynika z częstotliwości stosowania obecnie funkcjonujących w polskim porządku prawnym rozwiązań z art. 32c ustawy o ABW oraz AW.

> Art. 26g. 1. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej dostawca usług hostingowych jest obowiązany do dostarczenia Szefowi ABW, na każde jego żądanie, w terminie 30 dni od dnia otrzymania żądania danych niezbędnych do określenia podstawy wymiaru kary pieniężnej.
> 2. W przypadku niedostarczenia przez dostawcę usług hostingowych danych lub gdy dostarczone przez tego dostawcę dane uniemożliwiają ustalenie podstawy wymiaru kary pieniężnej Szef ABW ustala podstawę wymiaru tej kary w sposób szacunkowy, uwzględniając ogólnie dostępne dane finansowe dotyczące tego dostawcy, w tym kryteria, o których mowa w art. 7 ust. 1 pkt 1–3 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.

Art. 26g ustawy obliguje dostawcę usług hostingowych do współpracy z Szefem ABW w związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej. Niewykonanie obowiązku zawartego w ust. 1 lub dostarczenie danych, które uniemożliwiają ustalenie podstawy wymiaru kary, skutkuje tym, że Szef ABW ustala podstawę wymiaru tej kary w sposób szacunkowy, z uwzględnieniem ogólnie dostępnych danych finansowych dotyczących tego dostawcy, w tym kryteria, o których mowa

[40] *Rządowy projekt ustawy o zmianie ustawy...* – ocena skutków regulacji, https://orka.sejm.gov.pl/Druki10ka.nsf/0/5083CA680B1B465AC1258B97003B446F/%24File/661.pdf, s. 8 [dostęp: 14 XII 2024].

w ustawie – Prawo przedsiębiorców. Wspomniane kryteria to wielkość przedsiębiorstwa – czy jest on mikroprzedsiębiorcą, małym przedsiębiorcą czy średnim przedsiębiorcą.

Przepis ten jest analogiczny względem funkcjonującego w porządku prawnym art. 101a *Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych*.

> Art. 26h. Karę pieniężną uiszcza się w terminie 14 dni od dnia, w którym decyzja Szefa ABW, o której mowa w art. 26f ust. 2, stała się prawomocna.

Termin na uiszczenie kary pieniężnej to 14 dni liczone od dnia, w którym decyzja administracyjna Szefa ABW o nałożeniu kary pieniężnej stała się prawomocna, i jak wskazano, jest ona ostateczna.

Podsumowanie

Ustawą o zmianie ustawy o działaniach antyterrorystycznych i ustawy o ABW i AW przez nowelizację ustawy o działaniach antyterrorystycznych, w opinii autora, zostało zapewnione właściwe stosowanie rozporządzenia 2021/784. Wyznaczenie Szefa ABW jako polskiego właściwego organu w rozumieniu wyżej wskazanego rozporządzenia, a także ustanowienie punktu kontaktowego w kierowanej przez niego formacji jest optymalne z perspektywy usprawnienia funkcjonowania polskiego systemu antyterrorystycznego oraz jego podziału kompetencyjnego. Jako w pełni uzasadnione należy uznać również oparcie polskich przepisów proceduralnych, subsydiarnych względem przepisów rozporządzenia 2021/784, na rozwiązaniach przyjętych w k.p.a., przy jednoczesnym uznaniu, że w niektórych przypadkach mogą mieć zastosowanie tylko jego wybrane przepisy.

Mimo to w opinii autora do ustawy o działaniach antyterrorystycznych powinny zostać przeniesione wszystkie przepisy mające znaczenie z perspektywy przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, a zatem art. 32c ustawy o ABW oraz AW. Zabieg ten miałby jednak wymiar jedynie legislacyjny, ponieważ te regulacje zawierają normy kolizyjne gwarantujące spójność ich stosowania.

Zapewnienie stosowania rozporządzenia 2021/784 przez nowelizację ustawy o działaniach AT, w kontekście legislacyjnym, powinno zostać uzupełnione o modyfikację art. 1 tej ustawy, zgodnie z którym określa ona

zasady prowadzenia działań antyterrorystycznych (zatem działań administracji publicznej) oraz współpracy między organami właściwymi w zakresie prowadzenia tych działań. Rozwiązania przyjęte w nowym rozdziale 5a tej ustawy służące przeciwdziałaniu rozpowszechnianiu w internecie treści o charakterze terrorystycznym, zwłaszcza w kontekście będących ich skutkiem praw i obowiązków dostawców usług hostingowych i dostawców treści, powinny znaleźć odzwierciedlenie w przepisie określającym zakres regulacji.

Z perspektywy praktycznej zapewnienie stosowania rozporządzenia 2021/784 można ocenić jako wzmocnienie polskiego systemu antyterrorystycznego. W tym kontekście warto odnotować, że od 3 lipca 2023 r. funkcjonuje opracowana przez Europol platforma PERCI. Jest to rozwiązanie oparte na chmurze, zapewniające bezpieczeństwo i ochronę zamieszczanych w niej danych. Platforma ta 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[41].

W powyższym kontekście należy zauważyć, że choć zgodnie z rozporządzeniem 2021/784 państwa powinny zapewnić jego stosowanie od 7 czerwca 2022 r., to w Polsce nastąpiło to dopiero 3 grudnia 2024 r. Do tego czasu Polska była pozbawiona zarówno formalnych podstaw stosowania rozporządzenia, jak i możliwości korzystania z narzędzi jego wsparcia technicznego. Kwestia ta pozostaje tym istotniejsza, że w tym okresie na terytorium Polski obowiązywały stopnie alarmowe związane z podwyższonym zagrożeniem o charakterze terrorystycznym[42].

Warto też przywołać na koniec motyw 2 rozporządzenia 2021/784, który wskazuje, że:

> środki regulacyjne mające przeciwdziałać rozpowszechnianiu w internecie treści o charakterze terrorystycznym powinny zostać uzupełnione strategiami państw członkowskich dotyczącymi walki z terroryzmem, obejmującymi między innymi wzmacnianie umiejętności korzystania z mediów i umiejętności krytycznego myślenia,

[41] *Rządowy projekt ustawy o zmianie ustawy*... – uzasadnienie..., s. 5.

[42] *Dotychczas wprowadzane stopnie alarmowe i stopnie alarmowe CRP na terytorium RP*, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/dotychczas-wprowadzane-stopnie-alarmowe-i-stopnie-alarmowe-crp-na-terytorium-rp [dostęp: 23 XII 2024].

> przedstawianie alternatywnych narracji lub kontrnarracji i inne inicjatywy służące zmniejszeniu wpływu umieszczanych w internecie treści o charakterze terrorystycznym i podatności na te treści, a także inwestycje w pracę społeczną, inicjatywy na rzecz deradykalizacji i kontakty z zainteresowanymi społecznościami, w celu wypracowania trwałego zapobiegania radykalizacji w społeczeństwie[43].

Tę wytyczną, choć niemającą charakteru obligatoryjnego, należy mieć na uwadze w kontekście przyszłej oceny stosowania przyjętych przepisów. Jeśli okaże się, że nakazy lub środki szczególne znajdą częste zastosowanie na poziomie krajowym, stanie się zasadne podjęcie dodatkowych działań o charakterze profilaktycznym.

Bibliografia

Burczaniuk P., *Zadania i uprawnienia organów ścigania karnego w zakresie zwalczania terroryzmu w Polsce – perspektywa prawna*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 9–30. https://doi.org/10.4467/27204383TER.22.017.16337.

Cichomski M., *Między konfliktem zbrojnym a terroryzmem państwowym – szczególne indywidualne środki ograniczające przyjęte w Polsce w kontekście wojny w Ukrainie i sytuacji w Białorusi. Perspektywa prawna*, „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 91–131. https://doi.org/10.4467/27204383TER.24.003.19391.

Cichomski M., Idzikowska-Ślęzak I., *Stopnie alarmowe – praktyczny i prawny wymiar ich stosowania*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 31–70. https://doi.org/10.4467/27204383TER.22.018.16338.

Cichomski M., Marchliński P., *Krajowe rozwiązania w zakresie bezpieczeństwa obrotu prekursorami materiałów wybuchowych – po zamachu terrorystycznym w Norwegii 22 lipca 2011 r. w kontekście nowych zadań Policji*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, s. 591–600.

Gabriel-Węglowski M., *Działania antyterrorystyczne. Komentarz*, Warszawa 2018.

[43] Motyw 2 rozporządzenia 2021/784.

Źródła internetowe

Dotychczas wprowadzane stopnie alarmowe i stopnie alarmowe CRP na terytorium RP, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/dotychczas-wprowadzane-stopnie-alarmowe-i-stopnie-alarmowe-crp-na-terytorium-rp [dostęp: 23 XII 2024].

List of national competent authority (authorities) and contact points, European Commission, 27 I 2025 r., 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?prefLang=pl [dostęp: 15 II 2025].

Punkt kontaktowy TCO, BIP ABW, https://bip.abw.gov.pl/bip/punkt-kontatowy-tco/525,Punkt-kontaktowy-TCO.html [dostęp: 13 XII 2024].

Akty prawne

Międzynarodowa Konwencja o poszukiwaniu i ratownictwie morskim, sporządzona w Hamburgu dnia 27 kwietnia 1979 r. (DzU z 1988 r. nr 27 poz. 184 i 185).

Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana) – (Dz. Urz. UE C 202/47 z 7 VI 2016 r.).

Traktat o Unii Europejskiej (wersja skonsolidowana) – (Dz. Urz. UE C 202/13 z 7 VI 2016 r.).

Rozporządzenie 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 172/79 z 17 V 2021 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 98/2013 z dnia 15 stycznia 2013 r. w sprawie wprowadzania do obrotu i używania prekursorów materiałów wybuchowych (Dz. Urz. UE L 39/1 z 9 II 2013 r.).

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 2005/671/WSiSW (Dz. Urz. UE L 88/6 z 31 III 2017 r.).

Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. Urz. UE L 241/1 z 17 IX 2015 r.).

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE L 218/8 z 14 VIII 2013 r.).

Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) – (Dz. Urz. L 178/1 z 17 VII 2000 r.).

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (t.j. DzU z 1997 r. nr 78 poz. 483, ze zm.).

Ustawa z dnia 18 października 2024 r. o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (DzU z 2024 r. poz. 1684).

Ustawa z dnia 26 lipca 2024 r. o zmianie niektórych ustaw w celu usprawnienia działań Sił Zbrojnych Rzeczypospolitej Polskiej, Policji oraz Straży Granicznej na wypadek zagrożenia bezpieczeństwa państwa (DzU z 2024 r. poz. 1248).

Ustawa z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (DzU z 2023 r. poz. 1834).

Ustawa z dnia 7 lipca 2023 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Prawo o ustroju sądów powszechnych, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (DzU z 2023 r. poz. 1860).

Ustawa z dnia 7 lipca 2023 r. o zmianie ustawy o ochronie żeglugi i portów morskich oraz niektórych innych ustaw (DzU z 2023 r. poz. 1489).

Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. DzU z 2024 r. poz. 507).

Ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa (DzU z 2022 r. poz. 583).

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (t.j. DzU z 2024 r. poz. 248, ze zm.).

Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (t.j. DzU z 2021 r. poz. 815, ze zm.).

Ustawa z dnia 21 stycznia 2021 r. o służbie zagranicznej (t.j. DzU z 2024 r. poz. 1691, ze zm.).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. DzU z 2019 r. poz. 1781).

Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (t.j. DzU z 2024 r. poz. 236, ze zm.).

Ustawa z dnia 6 marca 2018 r. – Przepisy wprowadzające ustawę – Prawo przedsiębiorców oraz inne ustawy dotyczące działalności gospodarczej (DzU z 2018 r. poz. 650).

Ustawa z dnia 26 stycznia 2018 r. – Przepisy wprowadzające ustawę o Straży Marszałkowskiej (DzU z 2018 r. poz. 730).

Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (DzU z 2018 r. poz. 138).

Ustawa z dnia 16 listopada 2016 r. – Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej (t.j. DzU z 2016 r. poz. 1948, ze zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (DzU z 2024 r. poz. 92, 1248, 1684).

Ustawa z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych (t.j. DzU z 2019 r. poz. 994).

Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. DzU z 2024 r. poz. 935, ze zm.).

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. DzU z 2024 r. poz. 812, ze zm.).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. DzU z 2022 r. poz. 902).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. DzU z 2024 r. poz. 17).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. DzU z 2024 r. poz. 145, ze zm.).

Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t.j. DzU z 2024 r. poz. 572).

Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (t.j. DzU z 2016 r. poz. 283).

Zalecenie Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie (Dz. Urz. L 63/50 z 6 III 2018 r.).

Orzecznictwo

Wyrok Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce, https://arch-bip.ms.gov.pl/pl/prawa-czlowieka/europejski-trybunal-praw-czlowieka/orzecznictwo-europejskiego-trybunalu-praw-czlowieka/listByYear,2.html?ComplainantYear=2024 [dostęp: 18 V 2025].

Inne dokumenty

Commission Staff Working Document Impact Assessment. Accompanying the document. Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12 IX 2018 r., SWD(2018) 408 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN [dostęp: 4 V 2023].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetów Regionów. Zwalczanie nielegalnych treści w internecie. W kierunku większej odpowiedzialności platform internetowych, Bruksela, 28 IX 2017 r., COM (2017) 555 final.

Mechanizmy blokowania w internecie treści o charakterze terrorystycznym w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, prezentacja Ministerstwa Spraw Wewnętrznych i Administracji, przygotowana na potrzeby Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych.

Rządowy projekt ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, druk nr 661, https://www.sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=661 [dostęp: 24 XII 2024].

Sprawozdanie Komisji Administracji i Spraw Wewnętrznych oraz Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii o rządowym projekcie ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (druk nr 661), druk nr 706, https://orka.sejm.gov.pl/Druki10ka.nsf/0/C75A45601BC82E4EC1258BB3003DFB3A/%24File/706.pdf [dostęp: 21 XII 2024].

Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania rozporządzenia (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, Bruksela, 14 II 2024 r., COM(2024) 64 final.

Stanowisko Komisji Europejskiej z 9 czerwca 2021 r. (sygn. INFR(2021)2046, C(2021)3630 final).

Mariusz Cichomski

Prawnik, socjolog. Zawodowo zajmuje się zagadnieniami związanymi z terroryzmem, przestępczością zorganizowaną, nadzorem nad działalnością służb, legislacją w zakresie bezpieczeństwa oraz sprawami dotyczącymi stosowania krajowych środków ograniczających. Autor ponad 30 publikacji z zakresu bezpieczeństwa, zwłaszcza w wymiarze prawnym, i socjologii.