ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4077

Studia nad Autorytaryzmem i Totalitaryzmem 43, nr 3
Wrocław 2021

https://doi.org/10.19195/2300-7249.43.3.24

EWA GALEWSKA
ORCID: 0000-0002-8444-0972
Uniwersytet Wrocławski
ewa.galewska@uwr.edu.pl

Problem z aktywnym poszukiwaniem w internecie treści o charakterze terrorystycznym. Uwagi na tle unijnego rozporządzenia

Słowa kluczowe: społeczeństwo demokratyczne, wolność słowa, treści terrorystyczne, dostawcy usług hostingowych.

PROBLEM WITH ACTIVE DETECTION OF TERRORISTIC CONTENT ONLINE: REMARKS IN THE LIGHT OF EU REGULATION

Abstract

The new EU regulation is aimed at fighting terroristic content online. Of particular importance are its provisions on special measures and assessment thereof in the light of the directive's provisions on hosting providers' liability for online content. EC's radical proposals in this respect raised serious doubts in the legislation procedure. The European Parliament and the Council intended to ensure the compliance of a regulation blueprint with the directive 2000/31/WE, therefore they proposed a variety of amendments to provisions on special measures. It is, however, doubtful that these guarantee a full coherence with the regime of hosting providers' liability. In order to tackle terroristic content effectively, it is necessary to transform the existing regime of hosting providers' liability that was established in the directive almost 20 years ago and does not respond to problems that we currently face.

Keywords: democratic society, freedom of speech, terroristic content, hosting service providers.

Wstęp

Przepisy rozporządzenia[1] są zaadresowane do między innymi dostawców usług hostingowych (dalej: dostawców), których dotyczą zasady ustanowione w dyrektywie[2]. Świadczą oni usługi społeczeństwa informacyjnego[3], czyli usługi normalnie świadczone za wynagrodzeniem, na odległość, drogą elektroniczną, na indywidualne żądanie odbiorcy, polegające na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek (art. 2 pkt 1 rozporządzenia). Przepisy rozporządzenia są nakierowane na treści o charakterze terrorystycznym[4] będące w istocie rodzajem informacji bezprawnych, o których mowa w dyrektywie[5]. Obejmują one materiały różnego rodzaju: tekst, obrazy, nagrania dźwiękowe i nagrania wideo, a także transmisje na żywo przestępstw terrorystycznych, które stwarzają niebezpieczeństwo popełnienia kolejnych takich przestępstw. Dla zidentyfikowania takich treści ważne jest przy tym, by materiały te podżegały lub nakłaniały kogoś do popełniania przestępstw terrorystycznych lub do przyczynienia się do ich popełniania, nakłaniały kogoś do uczestniczenia w działaniach grupy terrorystycznej lub pochwalały działalność terrorystyczną, w tym przez rozpowszechnianie materiałów przedstawiających atak terrorystyczny (pkt 11 rozporządzenia).

Spośród obowiązków, które w rozporządzeniu nałożono na dostawców, interesujące są zwłaszcza te dotyczące środków szczególnych, dlatego że ich idea zmieniła się w istotnym zakresie podczas postępowania legislacyjnego. W projekcie rozporządzenia KE[6] uczyniła z nich prawdziwy oręż, który miał służyć do aktywnego zwalczania treści terrorystycznych w internecie przez samych dostawców. Było to zresztą zgodne ze stanowiskiem tej instytucji wyrażanym już od kilku

[1] Rozporządzenie 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 r. (dalej: rozporządzenie).

[2] 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. UE L 178 z 17.07.2000 r. (dalej: dyrektywa).

[3] 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 241 z 17.09.2015 r., art. 1 lit. B.

[4] Zdefiniowanych w art. 2 pkt 7 rozporządzenia 2021/784.

[5] W artykule używane jest pojęcie informacji bezprawnych, stosownie do terminologii przyjętej w dyrektywie, albo treści, nielegalnych treści lub treści o charakterze terrorystycznym zgodnie z terminologią obecnie stosowaną w systemie prawa UE.

[6] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym. Wkład Komisji Europejskiej w spotkanie przywódców w Salzburgu w dniach 19–20 września 2018 r., COM (2018) 640 (dalej: Projekt rozporządzenia), s. 3

lat w aktach o charakterze niewiążącym[7]. Projekt nie był więc zaskoczeniem. Co istotne jednak, rozwiązania zaproponowane przez KE niejako „pomijały" istnienie zasad z dyrektywy będących fundamentami odpowiedzialności dostawców za treści udostępniane w internecie. Problem ten został zidentyfikowany przez pozostałe instytucje UE: PE i Radę, które zaproponowały wprowadzenie istotnych zmian w projekcie KE i tym samym pozbawiły go jego najważniejszych założeń.

Celem niniejszego artykułu jest analiza przepisów rozporządzenia w zakresie dotyczącym środków szczególnych i ich ocena w świetle przepisów dyrektywy dotyczących odpowiedzialności dostawców za treści zamieszczane w internecie. Pojawiają się pytania: czy KE słusznie zaproponowała tak daleko idące obowiązki dostawców w zakresie zwalczania treści o charakterze terrorystycznym? Czy instytucje UE miały rację, twierdząc, że propozycja KE nie jest zgodna z dyrektywą? Czy obecne przepisy rozporządzenia w zakresie dotyczącym środków szczególnych są w pełni zgodne z przepisami tej dyrektywy?

1. Dostawcy usług hostingowych i ich odpowiedzialność za treści o charakterze terrorystycznym w świetle przepisów dyrektywy

Dostawcy, o których mowa w rozporządzeniu, są objęci reżimem odpowiedzialności z dyrektywy jako podmioty świadczące usługi społeczeństwa informacyjnego, polegające na przechowywaniu informacji przekazanych przez usługobiorcę[8] (art. 14 ust. 1 dyrektywy). Stosownie do ustanowionych w niej zasad nie odpowiadają za treści zamieszczane przez użytkowników, o ile spełnione są określone warunki. Chodzi o to, by działalność dostawców miała charakter czysto techniczny, automatyczny i bierny, a zatem by nie mieli oni wiedzy o informacjach przekazywanych lub przechowywanych ani kontroli nad nimi (pkt 42 dyrektywy). Dostawcy nie ponoszą więc odpowiedzialności za informacje przechowywane na żądanie usługobiorcy pod warunkiem, że: a) nie posiedli wiarygodnych wiadomości o bezprawnym charakterze działalności lub informacji lub b) podejmują niezwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do informacji, gdy uzyskają takie wiadomości lub zostaną o nich powiadomieni (art. 14 ust. 1 dyrektywy). Innymi słowy przytoczone przepisy dyrektywy zabezpieczają dostawców przed odpowiedzialnością za nielegalne treści internetowe różnego rodzaju, o ile ich działalność ma charakter czysto techniczny, automa-

[7] Zob. E. Galewska, *Zwalczanie nielegalnych treści zamieszczanych przez użytkowników platform internetowych — kierunek regulacji Unii Europejskiej*, [w:] *Prawo nowych technologii*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, Warszawa 2021, s. 105 n.

[8] Więcej o pojęciu dostawców usług hostingowych E.I. Obergfell, A. Thamer, *(Non-) regulation of online platforms and internet intermediaries — the facts: Context and overview of the state of play*, „Journal of Intellectual Property Law and Practice" 12, 2017, nr 5, s. 438.

tyczny i bierny, a zatem nie mają wiedzy o bezprawnym charakterze informacji, a w razie jej powzięcia je usuwają[9]. Wyłączenie odpowiedzialności dostawców nie ma jednak wpływu na możliwość wydawania zakazów różnych typów, na przykład w formie orzeczeń sądów lub organów administracyjnych, nakazujących usunięcie lub zapobieżenie naruszeniu prawa łącznie z usunięciem bezprawnych informacji lub uniemożliwieniem dostępu do nich (art. 14 ust. 3 dyrektywy)[10].

W kontekście odpowiedzialności dostawców za treści zamieszczane w internecie istotne znaczenie ma zakaz nakładania ogólnego obowiązku w zakresie nadzoru oznaczający, że państwo członkowskie nie może ich zobowiązać w ogólny sposób do nadzorowania przekazywanych lub przechowywanych informacji ani do aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność (art. 15 ust. 1 dyrektywy). Zakaz ten obejmuje przede wszystkim sytuacje, w których na dostawcę nakładany jest obowiązek nadzorowania, na przykład przez system filtrowania, wszystkich lub zdecydowanej większości informacji, które przechowuje, jeżeli nadzór taki jest nieograniczony w czasie, obejmuje wszelkie przyszłe naruszenia i dotyczy treści nie tylko istniejących, ale także przyszłych[11]. Chodzi o to, aby dostawca, którego działanie ogranicza się do roli pośrednika, nie był zmuszony do prowadzenia nadzoru nad całością lub prawie całością treści wszystkich użytkowników jego usługi. W takiej sytuacji bowiem jego rola nie byłaby już neutralna, techniczna, automatyczna i bierna, a dostawca miałby świadomość przechowywanych informacji i sprawowałby nad nimi kontrolę, i w konsekwencji nie mógłby korzystać z wyłączenia odpowiedzialności[12].

Zakaz nakładania ogólnego obowiązku monitorowania wynikający z dyrektywy jest niejako łagodzony w jej punktach 46–48, w których zezwala się państwom członkowskim na wprowadzenie środków szczególnych w zakresie uprzedniego identyfikowania nielegalnych treści internetowych. Zakazuje się więc nakładania ogólnego obowiązku monitorowania nielegalnych treści, ale dopuszczalne są szczególne obowiązki w tym zakresie nakładane w prawie krajowym[13]. Oznacza to, że ogólne obowiązki nadzorowania informacji albo aktywnego poszukiwania faktów lub okoliczności wskazujących na bezprawną działalność są zakazane, ale dopuszcza się nakładanie obowiązków w zakresie nadzoru „mających zastosowanie do przypadków szczególnych". Za taki szczególny przypadek TSUE uznaje nakaz sądu, by dany dostawca zablokował dostęp do przechowywanych informacji, których treść jest identyczna do uprzednio uznanej za bezprawną, lub usunął taką informację, niezależnie od tego, kto wnioskował

[9] Wyrok Trybunału z dnia 23 marca 2010 r., C-236/08-238/08, ECLI:EU:C:2010:159, pkt 114.

[10] Wyrok Trybunału z dnia 3 października 2019 r., C-18/18, ECLI:EU:C:2019:821, pkt 24.

[11] Wyrok Trybunału z dnia 16 lutego 2012 r., C-360/10, ECLI:EU:C:2012:85, pkt 45.

[12] Opinia Rzecznika Generalnego w sprawie C-18/18, ECLI:EU:C:2019:458, pkt 35–36.

[13] K. Kaesling, *Privatising Law Enforcement in Social Networks: A comparative Model Analysis*, „Erasmus Law Review" 2018, nr 3, s. 154.

o przechowywanie tych informacji. Sąd może też nakazać dostawcy usunięcie informacji, których treść jest równoznaczna z treścią informacji uprzednio uznanej za mającą bezprawny charakter, lub zablokowanie dostępu do tych informacji, pod warunkiem że nadzorowanie i wyszukiwanie informacji, których dotyczy taki nakaz, jest ograniczone do informacji przekazujących wiadomość, której treść jest w istocie niezmieniona w porównaniu do treści, która doprowadziła do stwierdzenia bezprawności, i zawierających elementy określone w nakazie, oraz że różnice w sformułowaniu tej treści równoznacznej z treścią informacji uprzednio uznanej za mającą bezprawny charakter nie są tego rodzaju, by wymagać od dostawcy dokonania niezależnej oceny tej treści[14].

2. Od środków proaktywnych do środków szczególnych w przeciwdziałaniu treściom terrorystycznym w internecie

Jako cel projektu rozporządzenia KE wskazała zwiększenie skuteczności obecnych środków w zakresie wykrywania, identyfikacji i usuwania treści o charakterze terrorystycznym w internecie. Wyeksponowała przy tym rolę dostawców, podkreślając, że mają oni „szczególne obowiązki wobec społeczeństwa w zakresie ochrony swoich usług przed wykorzystaniem przez terrorystów i udzielania pomocy w przeciwdziałaniu rozpowszechniania w internecie, za pośrednictwem ich usług, treści o charakterze terrorystycznym". Takie stanowisko i będące niejako jego konsekwencją rozwiązania zaproponowane w projekcie rozporządzenia wpisują się w prezentowane już od dłuższego czasu[15] oczekiwanie KE, że dostawcy jeszcze bardziej zaangażują się w aktywne poszukiwanie nielegalnych treści. Na konieczność „bardziej aktywnego" wykrywania treści o charakterze terrorystycznym KE wskazała w wielu miejscach projektu rozporządzenia. Używała przy tym, podobnie jak w wielu innych dokumentach, określenia „środki proaktywne", niejako determinując tym samym ich charakter i zakres. Do takich środków zaliczyła automatyczne narzędzia do wykrywania, czyli technologie filtrujące, uznając je za istotny element zwalczania treści terrorystycznych w internecie ze względu na skalę i tempo niezbędne do ich skutecznego identyfikowania i usuwania[16].

Używana przez KE nazwa „proaktywność" sugeruje oczekiwanie podjęcia określonych działań przez dostawców, z własnej inicjatywy, po dokonaniu samodzielnej oceny pewnych treści. Rozwiązanie to zakłada więc dużą uznaniowość ze strony takich podmiotów, począwszy od podejmowania działań służących do zidentyfikowania takich treści, ich poszukiwania, a następnie ich oceny i podejmowania decyzji, czy należy je usunąć. Taki kierunek działań legislacyjnych

[14] C-18/18, pkt 34–37, 42–46, 53.

[15] Wyrażone na przykład w zaleceniu Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w Internecie, Dz. Urz. UE L 63.

[16] Projekt rozporządzenia, s. 2, 6, 20.

byłby sprzeczny z celami dyrektywy[17], prowadziłby bowiem do sytuacji, w której ustanowiony w niej system odpowiedzialności dostawców w praktyce przestałby działać wskutek podejmowanych przez nich działań na podstawie przepisów projektu rozporządzenia. Warto przy tym dodać, że KE w projekcie rozporządzenia starała się wykluczyć pewien automatyzm stosowania środków proaktywnych. Decyzję o ich zastosowaniu, i jak się wydaje rodzaj oraz zakres, pozostawiła dostawcy, który przed jej podjęciem miał ocenić zagrożenie i poziom narażenia na treści o charakterze terrorystycznym, a także wpływ na prawa osób trzecich i interes publiczny danych informacji. Na tej podstawie miał określić, jakie odpowiednie, skuteczne i proporcjonalne proaktywne środki należy wdrożyć[18].

Projekt rozporządzenia w wersji zaproponowanej przez KE budził wiele wątpliwości, ponieważ prowadził do poważnego wyłomu w reżimie odpowiedzialności dostawców za treści zamieszczane przez użytkowników. Wbrew zasadom wynikającym z dyrektywy nakładał na nich obowiązek aktywnego poszukiwania treści o charakterze terrorystycznym i prowadził do ogólnego obowiązku ich monitorowania. Środki proaktywne wskazane w projekcie rozporządzenia miały być podejmowane przez wszystkich dostawców decydujących o ich charakterze i zakresie. W ten sposób zyskiwali oni szczególny statusu podmiotu prywatnego dysponującego środkami w istotny sposób wpływającymi na prawa podstawowe.

Parlament Europejski, starając się złagodzić dość radykalne stanowisko KE, zaproponował zmianę nazwy ze środków proaktywnych na środki szczególne, czyli na przykład: regularne sprawozdania dla właściwych organów, zwiększenie zasobów ludzkich zajmujących się środkami ochrony usług przed publicznym rozpowszechnianiem treści o charakterze terrorystycznym oraz wymianę najlepszych praktyk[19]. Przepisy rozporządzenia w zakresie dotyczącym stosowania środków szczególnych zostały bardzo złagodzone w porównaniu do zaproponowanych przez KE. Zasadniczą zmianą jest to, że obowiązek ich stosowania przez dostawcę został powiązany (uzależniony od) z uprzednim działaniem odpowiedniego organu państwa członkowskiego. Taki organ powinien stwierdzić w drodze decyzji, że dostawca jest narażony na treści o charakterze terrorystycznym, i powiadomić go o tym (art. 5 ust. 4 rozporządzenia). Tylko wówczas aktualizują się jego obowiązki w zakresie stosowania środków szczególnych. Decyzja ta przy tym, jak wymaga prawodawca, powinna być oparta „na obiektywnych czynnikach, takich jak fakt otrzymania przez dostawcę co najmniej dwóch ostatecznych

[17] Równie krytycznie przedstawiciele doktryny odnosili się do innych inicjatyw KE o podobnych założeniach. Zob. choćby M.L. Montagnani, A. Trapova, *New Obligations for Internet Intermediaries in the Digital Single Market — Safe Harbours in Turmoil?*, „Journal of Internet Law" 22, 2019, nr 7, s. 3; K. Kaesling, *op. cit.*, s. 162.

[18] Projekt rozporządzenia, s. 20.

[19] Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 17 kwietnia 2019 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, P8_TA(2019)0421_, COM (2018) 0640 , s. 20.

nakazów usunięcia w ciągu ostatnich 12 miesięcy". Wymóg ten oznacza, że niepożądane są jakiekolwiek subiektywne oceny ze strony organu państwowego dotyczące ewentualnego narażenia dostawcy na treści o charakterze terrorystycznym. Warto jednak wskazać na to, że wprawdzie prawodawca podkreśla, że decyzja powinna być oparta na obiektywnych czynnikach i nawet przykład takiego czynnika podaje, ale wybór pozostałych pozostawia organowi państwa, co może prowadzić do nadużyć w tym zakresie i ewentualnej dyskryminacji poszczególnych dostawców.

Z przepisów art. 5 ust. 2 i 4 rozporządzenia wynika, że tylko dostawca, który otrzymał decyzję organu państwa o narażeniu na treści terrorystyczne, ma obowiązek stosowania środków szczególnych w celu ochrony swoich usług przed publicznym rozpowszechnianiem treści o charakterze terrorystycznym. Decyzja co do wyboru dodatkowych środków szczególnych pozostaje w gestii dostawcy i warto zauważyć, że katalog takich środków, których zastosowanie dopuszcza prawodawca, jest bardzo duży i sformułowany niezwykle ogólnie, jak się wydaje po to, by nie wprowadzać tu ograniczeń. Środki takie mogą obejmować: a) odpowiednie 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; b) łatwo dostępne i przyjazne dla użytkownika mechanizmy umożliwiające użytkownikom zgłaszanie lub sygnalizowanie dostawcy domniemanych treści o charakterze terrorystycznym; c) inne mechanizmy zwiększające świadomość na temat dostępności treści o charakterze terrorystycznym w ramach świadczonych przez niego usług, takie jak mechanizmy służące moderowaniu użytkowników; d) inne środki, które dostawca uzna za stosowne, by przeciwdziałać dostępności treści o charakterze terrorystycznym w ramach świadczonych przez niego usług (art. 5 ust. 2).

Jak się wydaje, pewną próbą zapewnienia zgodności z dyrektywą oraz wyważenia roli dostawców w zakresie identyfikowania i usuwania treści o charakterze terrorystycznym a koniecznością ochrony praw podstawowych są przepisy art. 5 ust. 3 rozporządzenia. Stosownie do nich środki szczególne muszą spełniać wszystkie następujące wymogi: a) skutecznie zmniejszać poziom narażenia usług dostawcy na treści o charakterze terrorystycznym; b) być ukierunkowane i proporcjonalne, uwzględniając w szczególności, jak duży jest poziom narażenia usług dostawcy na treści o charakterze terrorystycznym, a także zdolności techniczne i operacyjne, kondycję finansową, liczbę użytkowników jego usług oraz ilość dostarczanych przez nich treści; c) być stosowane w sposób, który uwzględnia pełne poszanowanie praw i uzasadnionego interesu użytkowników, w szczególności praw podstawowych dotyczących wolności wypowiedzi i informacji, poszanowania życia prywatnego i ochrony danych osobowych; d) być stosowane w staranny i niedyskryminacyjny sposób. Gdy środki szczególne wiążą się ze stosowaniem środków technicznych, należy wprowadzić odpowiednie i skuteczne

zabezpieczenia, w szczególności przez nadzór i weryfikację dokonywane przez człowieka, aby zapewnić dokładność i uniknąć usuwania materiałów, które nie tworzą treści o charakterze terrorystycznym.

Prawodawca uszczegóławia wskazane wymogi w preambule rozporządzenia, podkreślając, że dostawcy powinni przyjmować wyłącznie środki, które są konieczne, odpowiednie i proporcjonalne w społeczeństwie demokratycznym, uwzględniając szczególne znaczenie, jakie przyznano wolności wypowiedzi i informacji oraz wolności i pluralizmowi mediów. Środki, które mają wpływ na wolność wypowiedzi i informacji, powinny być ściśle ukierunkowane na przeciwdziałanie rozpowszechnianiu w internecie treści o charakterze terrorystycznym, przy poszanowaniu prawa do zgodnego z prawem otrzymywania i przekazywania informacji, z uwzględnieniem centralnej roli dostawców w ułatwianiu debaty publicznej oraz w rozpowszechnianiu i pozyskiwaniu faktów, opinii i idei zgodnie z prawem. Skuteczne środki internetowe służące przeciwdziałaniu treściom o charakterze terrorystycznym w internecie oraz ochrona wolności wypowiedzi i informacji nie mają sprzecznych celów, lecz uzupełniają się i wzajemnie się wzmacniają (pkt 10).

Środki szczególne, które dostawca zastosował lub zamierza zastosować, podlegają ocenie przez organ państwa członkowskiego w świetle ich zgodności z art. 5 ust. 2 i 3 rozporządzenia. Oceniając ich skuteczność i proporcjonalność, właściwe organy powinny uwzględnić odpowiednie parametry, w tym liczbę nakazów usunięcia wydanych wobec dostawcy, jego rozmiary i zdolność ekonomiczną oraz wpływ jego usług na rozpowszechnianie treści o charakterze terrorystycznym, na przykład na podstawie liczby użytkowników w UE, a także zabezpieczenia wprowadzone w celu przeciwdziałania wykorzystywaniu jego usług do rozpowszechniania w internecie treści o charakterze terrorystycznym (pkt 24 rozporządzenia). Jeżeli właściwy organ uzna, że podjęte środki szczególne nie są zgodne z wymogami z art. 5 ust. 2 i 3 rozporządzenia, zobowiązuje dostawcę do podjęcia dodatkowych niezbędnych środków w celu zapewnienia zgodności z tymi przepisami. Takie żądanie nie powinno prowadzić do nałożenia ogólnego obowiązku w zakresie nadzoru ani aktywnego poszukiwania faktów w rozumieniu dyrektywy, ani obowiązku stosowania zautomatyzowanych narzędzi (pkt 25 rozporządzenia). Nadal jednak to dostawca decyduje, jaki rodzaj środków szczególnych podejmie (art. 5 ust. 6 rozporządzenia), co jest wyrazem zasady dobrowolności podkreślanej przez prawodawcę unijnego[20].

Do oceny rozwiązań przyjętych w rozporządzeniu odnośnie do środków szczególnych ważne jest też to, że organ państwa członkowskiego decyduje nie tylko o konieczności zastosowania takich środków przez wydanie decyzji

[20] Przeciwdziałanie treściom o charakterze terrorystycznym w internecie to element większego problemu dotyczącego treści nielegalnych w internecie i wymaga połączenia środków o charakterze prawodawczym, nieprawodawczym i środków dobrowolnych, opartych na współpracy między organami a dostawcami usług hostingowych, w sposób, który w pełni szanuje prawa podstawowe.

o narażeniu na treści terrorystyczne, ocenia konkretne środki, i w dość istotny sposób wpływa na to, jakie środki zostaną ostatecznie zastosowane, ale też decyduje o niejako „zwinięciu" regulacji. Dostawca może bowiem zwrócić się do niego z wnioskiem o zmianę lub uchylenie decyzji o narażeniu na treści terrorystyczne, a organ, reagując na ów wniosek, opierając się na obiektywnych czynnikach, podejmuje decyzję w tej sprawie (art. 5 ust. 7 rozporządzenia), co jak się wydaje, odzwierciedla dążenie prawodawcy do zapewnienia „czasowego" charakteru omawianych tu obowiązków.

Podsumowanie

Oczekiwanie KE wyrażone w projekcie rozporządzenia, by dostawcy aktywniej poszukiwali treści o charakterze terrorystycznym, prowadziłoby do sytuacji, w której chcąc zrealizować nałożone na nich obowiązki, byliby zmuszeni, wbrew zasadzie z art. 15 dyrektywy, do nadzorowania treści zamieszczanych przez wszystkich użytkowników. Następnie, aby uniknąć odpowiedzialności, stosownie do przepisów art. 14 dyrektywy, usuwaliby wszelkie treści, nie analizując nawet dokładnie ich kontekstu. Wprawdzie, będąc tego świadoma, KE w projekcie rozporządzenia podkreśliła, że nie powinno ono prowadzić do utraty przez dostawców zwolnienia od odpowiedzialności, a nakładane na nich obowiązki nie mogą oznaczać ogólnego obowiązku nadzorowania. Co bardzo ważne, jednak sama dążyła do przełamania tej istotnej zasady, wprost dopuszczając odstępstwo od niej, na mocy rozporządzenia powołując się na poważne zagrożenia związane z rozpowszechnianiem treści o charakterze terrorystycznym[21]. Podczas procesu legislacyjnego słusznie wytykano KE, że przedstawiony projekt prowadzi w istocie do nakładania obowiązków sprzecznych z dyrektywą[22]. W konsekwencji jego założenia w zakresie dotyczącym środków służących identyfikowaniu i usuwaniu treści o charakterze terrorystycznym zostały znacznie zmienione.

Ostatecznie w rozporządzeniu ustanowiono zasadę, że wymóg podjęcia środków szczególnych pozostaje bez uszczerbku dla art. 15 ust. 1 dyrektywy i nie pociąga za sobą ogólnego obowiązku w zakresie nadzoru ani ogólnego obowiązku aktywnego poszukiwania faktów lub okoliczności wskazujących na bezprawną działalność (art. 5 ust. 8). Z kolei do odpowiedzialności dostawców w świetle art. 14 dyrektywy odniesiono się wyłącznie w preambule rozporządzenia, podkreślając, że podjęte przez nich środki szczególne „nie powinny same w sobie" prowadzić do utraty ze zwolnienia od odpowiedzialności (pkt 7). Można się jednak zastanawiać, czy takie zastrzeżenia wystarczą. Warto w tym kontekście pamiętać,

[21] Projekt rozporządzenia, s. 3.

[22] Sprawozdanie w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym, P8_A(2019)0193, COM (2018) 0640, s. 84.

że dostawca jest podmiotem szczególnym, to jest udostępnia swoje usługi innym podmiotom, które dzięki nim mogą dzielić się wytworzonymi przez siebie treściami. Sam dostawca nie uczestniczy w wytwarzaniu treści, to zadanie użytkowników, z reguły nie ma pełnej wiedzy, bo byłoby to niemożliwe z powodów technicznych, o treściach, które przekazuje w ramach swoich usług.

Reżim odpowiedzialności z dyrektywy zakłada, że bierna postawa dostawców w zakresie udostępniania informacji w ramach świadczonych usług wyklucza ich odpowiedzialność. Bierność tę można przełamać, przekazując dostawcy wiadomość o bezprawnym charakterze udostępnianych treści. W takiej sytuacji, aby utrzymać wyłączenie odpowiedzialności, dostawca powinien podjąć określone działania w celu ich usunięcia lub zablokowania. Zasada ta opiera się na założeniu, że jakiś podmiot publiczny lub prywatny przekazuje wiedzę o bezprawności pewnych informacji udostępnianych przez dostawcę, a ten podejmuje odpowiednie działania. W przepisach dyrektywy nie wykluczono jednak sytuacji, w której wspomnianą wiedzę dostawca pozyskuje z własnej inicjatywy. Nie można go jednak zobowiązać do ogólnego monitorowania ani do aktywnego wyszukiwania bezprawnych informacji.

Prawodawca unijny skonstruował przepisy rozporządzenia odmiennie, niż zakładała KE, uzależniając nałożenie obowiązków w zakresie stosowania środków szczególnych, służących w istocie identyfikowaniu treści o charakterze terrorystycznym, od uprzedniej decyzji organu państwa, a zatem ograniczając je podmiotowo (do niektórych dostawców) i czasowo (do czasu cofnięcia decyzji). Przepisy te jednak nie wykluczają nadzorowania wszystkich treści przez dostawcę, który jest adresatem takiej decyzji, a zatem można mieć wątpliwości, czy w istocie jej wydanie nie prowadzi do obowiązku ogólnego monitorowania. Wymaga bowiem od niego analizowania wszystkich treści i identyfikowania tych, które mają charakter terrorystyczny. To z kolei pozbawia go neutralnej roli w rozumieniu art. 14 ust. 1 dyrektywy i prowadzi do utraty zwolnienia z odpowiedzialności[23]. Widać wyraźnie, że decyzje z art. 5 rozporządzenia prawodawca uznaje za działania dopuszczone mocą art. 14 ust. 3 dyrektywy, czyli obowiązki mające zapobiegać naruszeniu, które wymagają nadzoru nad treściami, ale wyłącznie w sytuacjach szczególnych, a nie prowadzą do nadzoru o ogólnym charakterze. Wydaje się jednak, że nie wystarczy powiązać obowiązków z art. 5 rozporządzenia z decyzją organu państwowego, nawet jeżeli jest ona skierowana wyłącznie do określonych dostawców i ograniczona w czasie. Mimo to przepisy te nadal mogą prowadzić do ogólnego obowiązku w zakresie nadzoru, gdyby bowiem miały dotyczyć szczególnego przypadku, obowiązek nadzoru powinien być ograniczony co do przedmiotu i okresu trwania nadzoru. W takiej decyzji należałoby więc uwzględnić długość tego nadzoru oraz szczegółowych danych dotyczące charakteru odnośnych naruszeń, ich sprawcy i przedmiotu. Wszystkie

[23] Opinia Rzecznika Generalnego, C-18/18, pkt 38–39, 41.

te elementy są wzajemnie od siebie zależne i nawzajem powiązane[24]. Chodzi tu więc o takie, wystarczająco konkretne, określenie naruszenia, że obowiązek zidentyfikowania — pośród informacji pochodzących od jednego użytkownika — informacji identycznych lub o treści porównywalnej z tą, która została uznana za niezgodną z prawem, nie stanowi ogólnego obowiązku w zakresie nadzoru[25]. Takiego wymogu nie będą spełniały, ze względu na ich zbyt ogólny charakter, decyzje wydane na podstawie art. 5 rozporządzenia.

Istnieje bardzo duże prawdopodobieństwo, że dostawcy, do których zostaną skierowane decyzje wydane na podstawie art. 5 rozporządzenia, zostaną w pewien sposób automatycznie wykluczeni z kręgu podmiotów zwolnionych od odpowiedzialności zgodnie z art. 14 dyrektywy. Taki wniosek wynika chociażby z interpretacji TSUE, który jako element podlegający ocenie, czy dany podmiot podlega zwolnieniu z odpowiedzialności, wskazuje jego należytą staranność w stwierdzeniu bezprawności informacji[26]. Można więc uznać, że dostawcy, którzy zostali powiadomieni o tym, że są narażeni na treści o charakterze terrorystycznym, powinni, wykazując należytą staranność, rozpocząć ich aktywne poszukiwanie w celu ich usunięcia, albowiem tym samym ich działalność utraciła bierny i wyłącznie techniczny charakter. Takie powiadomienie oznacza bowiem w świetle przepisów rozporządzenia, że dostawca jest zmuszony do analizowania różnych treści zamieszczanych przez użytkowników w celu wychwycenia tych, które mają charakter terrorystyczny. Należy przy tym podkreślić, że to zadanie dostawców nie jest proste, oceniając bowiem, czy materiały są treściami o charakterze terrorystycznym, powinni uwzględniać na przykład charakter i treść komunikatów, kontekst, w jakim komunikaty te zostały przedstawione, oraz to, w jakim stopniu mogą one spowodować szkodliwe skutki dla bezpieczeństwa i ochrony osób (pkt 11 rozporządzenia). Dodatkowo w rozporządzeniu zastrzeżono, że materiałów publicznie rozpowszechnianych w celach edukacyjnych, dziennikarskich, artystycznych lub badawczych lub w celach zapobiegania terroryzmowi lub zwalczania terroryzmu, w tym materiałów służących wyrażaniu polemicznych lub kontrowersyjnych poglądów w ramach debaty publicznej, nie uznaje się za treści o charakterze terrorystycznym. W drodze oceny ustala się, jaki jest rzeczywisty cel danego rozpowszechniania i czy materiały są publicznie rozpowszechniane do tych celów (art. 1 ust. 3). Oznacza to, że gdy treść nie ma w sposób oczywisty charakteru terrorystycznego, dostawca będzie musiał dokonać jej dogłębnej analizy i uznać, czy spełnia ona warunki określone w rozporządzeniu, a zatem czy należy ją usunąć, jednocześnie odpowiednio wyważając prawa podstawowe. Wszystkie te działania, których podjęcia oczekuje się od dostawcy, wymagają wyspecjalizowanej wiedzy nie tylko prawniczej, lecz także

[24] *Ibidem*, pkt 44–47, 49–50.
[25] *Ibidem*, pkt 57, 58, 62.
[26] Wyrok Trybunału z dnia 12 lipca 2011 r., C-324/09, ECLI:EU:C:2011:474, pkt 120–122.

takiej, która pozwala na dokonanie oceny, czy dana treść jest w istocie treścią o charakterze terrorystycznym, czy też na przykład jest to udział w debacie publicznej. Nie wszyscy dostawcy dysponują odpowiednimi ku temu zasobami.

Można więc uznać, że jeżeli w UE będą obowiązywały zasady ustanowione dyrektywą jakiekolwiek próby wprowadzenia regulacji dotyczących zwalczania nielegalnych treści przez dostawców, będą wzbudzały wątpliwości. Samo „zaklinanie rzeczywistości" przez wskazywanie, że wprowadzane regulacje nie wpływają na zasady ustanowione w dyrektywie, nie jest wystarczające. Do zapewnienia efektywnego zwalczania treści o charakterze terrorystycznym konieczne jest istotne przeobrażenie istniejącego reżimu odpowiedzialności dostawców ustanowionego w dyrektywie ponad 20 lat temu i nieprzystającego do współczesnych problemów.

Bibliografia

Galewska E., *Zwalczanie nielegalnych treści zamieszczanych przez użytkowników platform internetowych — kierunek regulacji Unii Europejskiej*, [w:] *Prawo nowych technologii*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, Warszawa 2021.

Kaesling K., *Privatising Law Enforcement in Social Networks: A comparative Model Analysis*, „Erasmus Law Review" 2018, nr 3.

Montagnani M.L., Trapova A., *New Obligations for Internet Intermediaries in the Digital Single Market — Safe Harbours in Turmoil?*, „Journal of Internet Law" 22, 2019, nr 7.

Obergfell E.I., Thamer A., *(Non-) regulation of online platforms and internet intermediaries — the facts: Context and overview of the state of play*, „Journal of Intellectual Property Law and Practice" 12, 2017, nr 5.

Akty prawne

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. UE L 178 z 17.07.2000 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 241 z 17.09.2015 r.

Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 17 kwietnia 2019 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, P8_TA(2019)0421_, COM (2018) 0640.

Rozporządzenie 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 r.

Sprawozdanie w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym, P8_A(2019)0193, COM (2018) 0640.

Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w internecie treści i charakterze terrorystycznym. Wkład Komisji Europejskiej w spotkanie przywódców w Salzburgu w dniach 19–20 września 2018 r., COM (2018) 640.
Zalecenie Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w Internecie, Dz. Urz. UE L 63.
Opinia Rzecznika Generalnego w sprawie C-18/18, ECLI:EU:C:2019:458.
Wyrok Trybunału z dnia 23 marca 2010 r., C-236/08-238/08, ECLI:EU:C:2010:159.
Wyrok Trybunału z dnia 12 lipca 2011 r., C-324/09, ECLI:EU:C:2011:474.
Wyrok Trybunału z dnia 16 lutego 2012 r., C-360/10, ECLI:EU:C:2012:85.
Wyrok Trybunału z dnia 3 października 2019 r., C-18/18, ECLI:EU:C:2019:821.