KOMISJA
EUROPEJSKA

Bruksela, dnia 14.2.2024 r.
COM(2024) 64 final

SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO I RADY

z wykonania rozporządzenia (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym

{SWD(2024) 36 final}

1. STRESZCZENIE

Rozporządzenie (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym zapewnia państwom członkowskim ramy prawne na szczeblu europejskim w celu ochrony obywateli przed narażeniem na materiały o charakterze terrorystycznym w internecie. Rozporządzenie ma zapewnić sprawne funkcjonowanie jednolitego rynku cyfrowego przez przeciwdziałanie wykorzystywaniu usług hostingowych do publicznego rozpowszechniania w internecie treści o charakterze terrorystycznym. Jego celem jest zapobieganie wykorzystywaniu internetu przez terrorystów do szerzenia ich przesłania w celu zastraszenia, radykalizacji, rekrutacji i ułatwiania ataków terrorystycznych. Jest to szczególnie istotne w chwili obecnej, w kontekście konfliktów i niestabilności, które mają wpływ na bezpieczeństwo Europy. Rosyjska wojna napastnicza przeciwko Ukrainie i atak terrorystyczny przeprowadzony przez Hamas na Izrael 7 października 2023 r. doprowadziły do zwiększenia skali rozpowszechniania w internecie treści o charakterze terrorystycznym.

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.

Rozporządzenie w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym weszło w życie 7 czerwca 2022 r. Zgodnie z art. 22 rozporządzenia Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie ze stosowania rozporządzenia („sprawozdanie z wykonania").

Niniejsze sprawozdanie z wykonania sporządzono na podstawie oceny informacji otrzymanych od państw członkowskich, Europolu i dostawców usług hostingowych zgodnie z obowiązkami ustanowionymi w rozporządzeniu. Najważniejsze ustalenia dotyczące wykonania rozporządzenia sformułowane na podstawie tej oceny można podsumować w następujący sposób:

- Według stanu na dzień 31 grudnia 2023 r. **dwadzieścia trzy państwa członkowskie** wyznaczyły właściwy organ lub właściwe organy uprawnione do wydawania nakazów usunięcia zgodnie z rozporządzeniem[1]. Komisja udostępnia wykaz organów państw członkowskich na swojej stronie internetowej i regularnie go aktualizuje[2].

- Do 31 grudnia 2023 r. Komisja otrzymała informacje o co najmniej **349 nakazach usunięcia treści o charakterze terrorystycznym** wydanych przez właściwe organy sześciu państw członkowskich (Hiszpanii, Rumunii, Francji, Niemiec, Czech i Austrii), co

[1] Rejestr internetowy, utworzony przez Komisję zgodnie z art. 12 ust. 4 rozporządzenia, zawiera wykaz właściwych organów, o których mowa w art. 12 ust. 1, oraz punktów kontaktowych wyznaczonych lub ustanowionych zgodnie z art. 12 ust. 2 w ramach każdego właściwego organu. Rejestr jest regularnie aktualizowany na podstawie powiadomień otrzymywanych od państw członkowskich. Wykaz właściwych organów krajowych i punktów kontaktowych (europa.eu).

[2] Wykaz właściwych organów krajowych i punktów kontaktowych.

w większości przypadków doprowadziło do podjęcia przez dostawców usług hostingowych szybkich działań następczych w celu usunięcia treści o charakterze terrorystycznym lub zablokowania dostępu do nich. Stanowi to dowód na to, że narzędzia przewidziane w rozporządzeniu zaczynają być wykorzystywane i skutecznie zapewniają szybkie usuwanie treści o charakterze terrorystycznym przez dostawców usług hostingowych zgodnie z art. 3 ust. 3. Zgodnie z informacjami otrzymanymi przez Komisję wspomniane nakazy usunięcia nie zostały zaskarżone.

- Właściwe organy państw członkowskich i Europol, a mianowicie unijna jednostka ds. zgłaszania podejrzanych treści w internecie działająca w strukturach Europolu, **dobrze koordynują swoje działania** w zakresie stosowania rozporządzenia, w szczególności jeżeli chodzi o przetwarzanie nakazów usunięcia.
- 3 lipca 2023 r. Europol udostępnił narzędzie **PERCI**[3]. Narzędzie to było z powodzeniem wykorzystywane przez szereg państw członkowskich do przekazywania zarówno nakazów usunięcia, jak i zgłoszeń[4]. Właściwe organy Hiszpanii, Niemiec, Austrii, Francji i Czech korzystały z tego narzędzia do przekazywania nakazów usunięcia. Ogólnie rzecz biorąc, od uruchomienia PERCI w dniu 3 lipca do 31 grudnia 2023 r. za pomocą tego narzędzia przetworzono co najmniej 14 615 zgłoszeń.
- Chociaż w rozporządzeniu nie przewidziano żadnych szczególnych środków dotyczących zgłoszeń, z informacji otrzymanych przez Komisję wynika, że od momentu rozpoczęcia stosowania rozporządzenia odnotowano również **wzrost szybkości reagowania na zgłoszenia** ze strony dostawców usług hostingowych.
- Zgodnie z wiedzą posiadaną przez Komisję, do 31 grudnia 2023 r. nie określono żadnego dostawcy usług hostingowych jako narażonego na treści o charakterze terrorystycznym w rozumieniu art. 5 ust. 4 rozporządzenia. Takie wskazanie jest warunkiem wstępnym zastosowania środków szczególnych, o których mowa w tym artykule. Niemniej jednak, zgodnie ze sprawozdaniami z przejrzystości przedstawionymi przez dostawców usług hostingowych, wprowadzili oni środki w celu **przeciwdziałania wykorzystywaniu ich usług do rozpowszechniania treści o charakterze terrorystycznym**, w szczególności w drodze przyjęcia szczegółowych warunków umownych oraz stosowania innych przepisów i środków mających na celu ograniczenie rozpowszechniania treści o charakterze terrorystycznym.
- Dostawcy usług hostingowych wprowadzili również środki dotyczące powiadamiania o **bezpośrednim zagrożeniu życia** zgodnie z art. 14 ust. 5 rozporządzenia.

Jeżeli chodzi o **mniejszych dostawców usług hostingowych**, w 2021 r. Komisja ogłosiła zaproszenie do składania wniosków, aby wesprzeć ich w wykonywaniu rozporządzenia. Komisja udzieliła w 2022 r. zamówienia na trzy projekty (zob. sekcja 4.8), których realizację rozpoczęto

[3] PERCI *(Plateforme Européenne de Retraits des Contenus illégaux sur Internet*) to platforma służąca do usuwania nielegalnych treści w internecie opracowana i obsługiwana przez Europol. Ułatwia wykonywanie rozporządzenia, zapewniając rozwiązanie techniczne do przetwarzania zgłoszeń i nakazów usunięcia skierowanych do dostawców usług hostingowych, a także inne funkcje.

[4] Zgłoszenia są mechanizmem powiadamiania dostawców usług hostingowych o określonych treściach, aby dostawca usług mógł dobrowolnie rozważyć, czy są one zgodne z jego własnymi warunkami umownymi. W rozporządzeniu (motyw 40) stwierdzono, że zgłoszenia okazały się skutecznym narzędziem, które nadal powinno być dostępne w uzupełnieniu do nakazów usunięcia.

w 2023 r. i które przyniosły już pewne rezultaty, jeżeli chodzi o zapewnianie wsparcia małym przedsiębiorstwom w osiągnięciu zgodności z rozporządzeniem.

Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 22 państwom członkowskim w związku z niewyznaczeniem właściwych organów zgodnie z art. 12 ust. 1 rozporządzenia oraz niewypełnieniem obowiązków wynikających z art. 12 ust. 2, art. 12 ust. 3 i art. 18 ust. 1, wysyłając 26 stycznia 2023 r. **wezwania do usunięcia uchybienia**[5]. Po wszczęciu postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego kolejne państwa członkowskie zgłosiły właściwe organy odpowiedzialne za rozpatrywanie nakazów usunięcia, co odzwierciedlają informacje opublikowane w rejestrze internetowym[6]. Ponadto 11 postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego wszczętych w styczniu 2023 r. zamknięto do 21 grudnia 2023 r.[7].

Na podstawie informacji otrzymanych od państw członkowskich i Europolu oraz udostępnionych przez dostawców usług hostingowych Komisja stwierdziła, że stosowanie rozporządzenia miało **pozytywny wpływ** na ograniczenie rozpowszechniania w internecie treści o charakterze terrorystycznym.

2. KONTEKST

Rozporządzenie weszło w życie 7 czerwca 2022 r. Celem rozporządzenia jest zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego przez przeciwdziałanie wykorzystywaniu usług hostingowych do publicznego rozpowszechniania w internecie treści o charakterze terrorystycznym. Zapewnia on państwom członkowskim ukierunkowane narzędzia, w formie nakazów usunięcia, w celu przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, oraz umożliwia państwom członkowskim zwracanie się do dostawców usług hostingowych niezależnie od ich wielkości o podjęcie szczególnych środków w celu ochrony ich usług przed wykorzystywaniem przez podmioty terrorystyczne, gdy są one narażone na treści o charakterze terrorystycznym.

Ponadto wraz z wejściem w życie aktu o usługach cyfrowych 16 listopada 2022 r. otoczenie regulacyjne zostało rozszerzone przepisami horyzontalnymi o szerokim zakresie mającym na celu zapewnienie konsumentom bezpieczniejszej przestrzeni cyfrowej, skutecznych środków zwalczania nielegalnych treści i bardziej przejrzystych warunków świadczenia usług. Akt o usługach cyfrowych przyznaje Komisji szerokie uprawnienia nadzorcze, dochodzeniowe i wykonawcze do podejmowania działań skierowanych do bardzo dużych platform internetowych i wyszukiwarek internetowych. Działania te obejmują wnioski o udzielenie informacji i dochodzenia w sprawie działań przedsiębiorstw w zakresie moderowania treści z możliwością nakładania grzywien.

[5]Zob. komunikat prasowy: Treści o charakterze terrorystycznym w internecie (europa.eu).
[6] Wykaz właściwych organów krajowych i punktów kontaktowych (europa.eu). W rejestrze internetowym przedstawiono informacje o 23 organach państw członkowskich właściwych do wydawania nakazów usunięcia zgodnie z art. 12 ust. 1 lit. a).
[7]Finlandia, Malta, Czechy, Dania, Rumunia, Szwecja, Łotwa, Hiszpania, Litwa, Austria i Słowacja.

Akt o usługach cyfrowych umożliwia zwalczanie wszelkich form nielegalnych treści, umożliwiając Komisji żądanie od platform dostarczenia dowodów, że wywiązują się one ze swoich zobowiązań w zakresie usuwania treści. Natomiast rozporządzenie w sprawie treści o charakterze terrorystycznym w internecie stanowi jeszcze bardziej skuteczne narzędzie w odniesieniu do tej konkretnej formy nielegalnych treści, z prawnym obowiązkiem usunięcia treści w ciągu jednej godziny od otrzymania nakazu usunięcia oraz skutecznymi mechanizmami sankcji.

Jak podkreślił Europol w sprawozdaniach dotyczących sytuacji i tendencji w dziedzinie terroryzmu w UE (TE-SAT)[8] opublikowanych w ostatnich latach, terroryści intensywnie wykorzystują internet do szerzenia swoich przesłań w celu zastraszania, radykalizacji, rekrutacji i ułatwiania ataków terrorystycznych. 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[9], 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[10]. 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.

W art. 22 rozporządzenia zobowiązano Komisję do przedłożenia Parlamentowi Europejskiemu i Radzie sprawozdania ze stosowania rozporządzenia („sprawozdanie z wykonania") do 7 czerwca 2023 r., sporządzonego na podstawie informacji przekazanych przez państwa członkowskie, które z kolei częściowo oparły się na informacjach przekazanych przez dostawców usług hostingowych (art. 21). Opóźnienie w przedłożeniu sprawozdania z wykonania wynika z jednej strony z faktu, że państwa członkowskie i dostawcy usług hostingowych późno przesłali Komisji kluczowe informacje. Z drugiej strony Komisja uznała, że w sprawozdaniu z wykonania należy uwzględnić wykorzystanie narzędzia PERCI, które zaczęło funkcjonować 3 lipca 2023 r. i którego od tego czasu używa się do przetwarzania nakazów usunięcia zgodnie z rozporządzeniem.

Niniejsze sprawozdanie z wykonania ma jedynie na celu przedstawienie rzeczowego przeglądu istotnych kwestii związanych ze stosowaniem rozporządzenia. Nie zawarto w nim żadnych wykładni rozporządzenia ani opinii na temat wykładni lub innych środków podjętych w ramach stosowania rozporządzenia.

Zgodnie z art. 21 ust. 2 rozporządzenia do tego samego dnia (7 czerwca 2023 r.) Komisja musiała ustalić szczegółowy program monitorowania wyników, rezultatów i skutków rozporządzenia. W szczególności w programie monitorowania należy określić wskaźniki, środki i przedziały

[8] Sprawozdanie Europolu TE-SAT za 2023 r. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2023.pdf i za 2022 r. https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

[9] Komisja Europejska, (2018), Ocena skutków towarzysząca wnioskowi dotyczącemu rozporządzenia w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, SWD(2018) 408 final, dostęp z dnia 04.5.2023 r. pod adresem: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN.

[10] Tamże.

czasowe dotyczące gromadzenia danych i innych niezbędnych dowodów. Program taki ustanowiono w towarzyszącym dokumencie roboczym służb Komisji. Określono w nim działania, które Komisja i państwa członkowskie mają podjąć w ramach gromadzenia i analizowania danych i innych dowodów w celu monitorowania postępów i skutków rozporządzenia oraz przeprowadzenia oceny rozporządzenia zgodnie z jego art. 23.

3. CEL I METODYKA SPRAWOZDANIA

Celem niniejszego sprawozdania jest ocena stosowania rozporządzenia i jego dotychczasowego wpływu na ograniczenie rozpowszechniania w internecie treści o charakterze terrorystycznym. Obejmuje to działania podejmowane przez państwa członkowskie i dostawców usług hostingowych, takie jak zmiany warunków umownych i zasad społecznościowych oraz wykonywanie nakazów usunięcia i reagowanie na nie.

W tym celu Komisja zebrała informacje od państw członkowskich, unijnej jednostki ds. zgłaszania podejrzanych treści w internecie działającej w strukturach Europolu i dostawców usług hostingowych, w tym informacje zawarte w sprawozdaniach z przejrzystości i monitorowania sporządzonych na podstawie art. 7, 8 i 21 rozporządzenia. Informacje wymagane w art. 8 i 21 otrzymano od 18 państw członkowskich. Informacje na temat działań podjętych przez dostawców usług hostingowych zgromadzono za pośrednictwem ich rocznych sprawozdań z przejrzystości, Europolu oraz w ramach bezpośredniej dobrowolnej komunikacji ze służbami Komisji. Niniejsze sprawozdanie z wykonywania zawiera informacje otrzymane przez Komisję do 31 grudnia 2023 r.

Obowiązki w zakresie monitorowania i przejrzystości (art. 21, 7 i 8)

Zgodnie z art. 21 ust. 1 rozporządzenia w celu sporządzenia sprawozdania z wykonywania państwa członkowskie są zobowiązane do gromadzenia i przesyłania Komisji do 31 marca każdego roku informacji, które uzyskały od swoich właściwych organów i dostawców usług hostingowych podlegających ich jurysdykcji. Obejmuje to informacje na temat działań podjętych przez te organy i tych dostawców zgodnie z rozporządzeniem w poprzednim roku kalendarzowym. W art. 21 ust. 1 określono rodzaje informacji, które państwa członkowskie powinny gromadzić, dotyczących środków wprowadzonych w celu zapewnienia zgodności z rozporządzeniem; informacje te obejmują informacje szczegółowe na temat nakazów usunięcia, liczbę wniosków o dostęp do przechowywanych treści w celu umożliwienia prowadzenia postępowań przygotowawczych, informacje na temat procedur rozpatrywania skarg oraz kontroli administracyjnej i sądowej.

Zgodnie z art. 7 ust. 1 rozporządzenia dostawcy usług hostingowych określają w swoich warunkach umownych w sposób jasny swoje zasady dotyczące przeciwdziałania rozpowszechnianiu treści o charakterze terrorystycznym, w tym, w stosownych przypadkach, rzeczowe wyjaśnienie funkcjonowania środków szczególnych.

Ponadto zgodnie z art. 7 ust. 2 rozporządzenia 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 rozporządzenia, udostępnia publicznie ogólnie dostępne sprawozdanie z przejrzystości na temat

tych działań za ten rok. Powinien opublikować to sprawozdanie przed dniem 1 marca następnego roku.

W art. 7 ust. 3 rozporządzenia określono minimalny zakres informacji, które powinno się zawrzeć w tych sprawozdaniach z przejrzystości, np. dotyczące środków wprowadzonych w celu identyfikacji treści o charakterze terrorystycznym i uniemożliwienia dostępu do nich, liczby przypadków usunięcia treści lub ich przywrócenia oraz wyników skarg.

Zgodnie z art. 8 rozporządzenia wyznaczone właściwe organy państw członkowskich publikują roczne sprawozdania z przejrzystości dotyczące ich działalności prowadzonej na podstawie rozporządzenia. W art. 8 ust. 1 określono minimalny zakres informacji, które powinno się zawrzeć w tych sprawozdaniach[11].

Według stanu na dzień 31 grudnia 2023 r. osiemnaście państw członkowskich przesłało Komisji informacje na temat swoich działań podjętych zgodnie z rozporządzeniem, podczas gdy dwadzieścia trzy państwa członkowskie wyznaczyły właściwy organ lub właściwe organy uprawnione do wydawania nakazów usunięcia zgodnie z rozporządzeniem.

4. KONKRETNE ELEMENTY BĘDĄCE PRZEDMIOTEM OCENY

4.1. NAKAZY USUNIĘCIA (art. 3)

Łącznie do 31 grudnia 2023 r. Komisja otrzymała informacje o co najmniej 349 nakazach usunięcia wysłanych przez właściwe organy Hiszpanii, Rumunii, Francji, Niemiec, Austrii i Czech do następujących podmiotów: Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L., FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net oraz Catbox.

Hiszpański właściwy organ – CITCO (*Centro de Inteligencia contra el Terrorismo y el Crimen Organizado*) – wysłał 62 nakazy usunięcia, podczas gdy rumuński właściwy organ (ANCOM – Autoritatea Națională pentru Administrare și Reglementare în Comunicații) wysłał dwa nakazy usunięcia, a francuski właściwy organ (OCLCTIC - L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) wysłał 26 nakazów usunięcia. Od czasu ataku terrorystycznego przeprowadzonego przez Hamas na Izrael niemiecki właściwy organ (BKA – Bundeskriminalamt) wysłał 249 nakazów usunięcia.

Hiszpański właściwy organ przekazał 62 nakazy usunięcia: 18 przed uruchomieniem PERCI i 44 za pośrednictwem tego narzędzia. Przedstawił szczegółowy opis procesu przekazania pierwszych wydawanych nakazów usunięcia i podjętych w związku z nimi działań następczych, co jest bardzo istotne dla lepszego zrozumienia wpływu i skutków rozporządzenia.

Dwa pierwsze nakazy usunięcia hiszpański właściwy organ wydał 24 kwietnia 2023 r.[12] Dotyczyły one dwóch przypadków treści o charakterze terrorystycznym, z których jeden dotyczył terroryzmu

[11] Zob. art. 8 ust. 1 rozporządzenia (UE) 2021/784 https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32021R0784

[12] Ministerio del Interior | El CITCO culmina la retirada de Internet de dos contenidos que alentaban al terrorismo.

prawicowego, a drugi – dżihadyzmu. Pierwszy nakaz usunięcia dotyczył publicznie udostępnionego w serwisie Telegram dokumentu w formacie PDF, w którym nawoływano do przemocy terrorystycznej i gloryfikowano prawicowe ataki terrorystyczne. Drugi nakaz usunięcia treści o charakterze terrorystycznym dotyczył zamieszczonego w serwisie Internet Archive nagrania wideo przedstawiającego walczących dżihadystów z organizacji terrorystycznej znanej jako „Państwo Islamskie". Obie treści usunięto z obu platform w czasie krótszym niż jedna godzina, a więc zgodnie z art. 3 ust. 3 rozporządzenia. Hiszpański właściwy organ przedstawił ocenę, w której wyjaśnił, że zdecydował się na zastosowanie nakazu usunięcia, a nie zgłoszenia, z dwóch głównych powodów: zachowanie zgodności z wymogami rozporządzenia dotyczącymi nakazów usunięcia oraz pilny charakter spraw. Hiszpański właściwy organ wydał następnie kolejne nakazy usunięcia.

Organ hiszpański zwrócił uwagę na wyzwania związane z faktem, że jeden z dostawców usług hostingowych (Meta) wykorzystywał do przyjmowania nakazów usunięcia formularz internetowy, zamiast zapewnić bezpośredni punkt kontaktowy. Konieczność korzystania z formularza internetowego spowodowała również problemy z komunikacją z właściwym organem państwa członkowskiego, w którym znajduje się główna jednostka organizacyjna tego dostawcy usług hostingowych.

13 lipca 2023 r. francuski właściwy organ wydał pierwszy nakaz usunięcia skierowany do platformy wymiany informacji (Justpaste.it), która usunęła treści o charakterze terrorystycznym w ciągu jednej godziny. Nakaz dotyczył treści propagandowych Al-Kaidy, a dokładniej materiałów jej sekcji medialnej, Rikan Ka Mimber, z indyjskiego odłamu tej organizacji – Al-Kaida Subkontynentu Indyjskiego (AQIS). Pełne usunięcie treści potwierdzono na platformie Europolu PERCI.

16 października 2023 r. niemiecki właściwy organ wydał sześć nakazów usunięcia wymierzonych w propagandę Hamasu i Palestyńskiego Islamskiego Dżihadu, 18 października – 16 nakazów, a 24 października – pięć. Dostęp do tych treści w UE został zablokowany, zgodnie z art. 3 ust. 3 rozporządzenia. Niemiecki właściwy organ najpierw wysłał zgłoszenia, a gdy nie przyniosły one skutku, wydał nakazy usunięcia. Po ataku dokonanym przez Hamas 7 października 2023 r. niemiecki właściwy organ wysłał 249 nakazów usunięcia, głównie do serwisu Telegram[13].

Właściwy organ Republiki Czeskiej i właściwy organ Austrii wydały 2 i 8 nakazów usunięcia, odpowiednio do serwisów X i Telegram.

Organy hiszpańskie wskazały dwa problemy związane z faktem, że jeden z dostawców usług hostingowych przyjmował nakazy usunięcia za pośrednictwem formularza internetowego: 1) w kontekście art. 3 ust. 2 rozporządzenia formularz internetowy nie pozwala właściwym organom państw członkowskich na przesłanie dostawcy usług hostingowych informacji o mających zastosowanie procedurach i terminach przed wydaniem pierwszego nakazu usunięcia; 2) w kontekście art. 4 ust. 1 formularz internetowy nie umożliwia jednoczesnego przedłożenia kopii nakazu usunięcia właściwemu organowi państwa członkowskiego, w którym znajduje się główna

[13]Zgodnie z informacjami, którymi dysponuje Komisja.

jednostka organizacyjna dostawcy usług hostingowych, oraz przedstawicielowi prawnemu tego dostawcy.

4.2 TRANSGRANICZNE NAKAZY USUNIĘCIA (art. 4)

W przypadku dwóch pierwszych nakazów usunięcia wydanych w kwietniu 2023 r. hiszpański właściwy organ nie mógł przesłać kopii nakazu do organu państwa członkowskiego, w którym znajdowała się główna jednostka organizacyjna dostawcy usług hostingowych lub w którym przedstawiciel prawny tego dostawcy miał siedzibę, ponieważ żaden z tych dwóch dostawców usług hostingowych nie dysponował wówczas główną jednostką organizacyjną ani nie wyznaczył przedstawiciela prawnego w UE. W przypadku kolejnych nakazów usunięcia hiszpański właściwy organ przesłał kopie nakazów do właściwego organu państwa członkowskiego, w którym znajdowała się główna jednostka organizacyjna dostawcy usług hostingowych lub w którym dostawca ten wyznaczył swojego przedstawiciela prawnego.

Państwa członkowskie poinformowały, że przekazywanie nakazów usunięcia dostawcom usług hostingowych mających siedzibę w państwach trzecich, którzy nie wypełnili jeszcze obowiązku wyznaczenia przedstawicielstwa prawnego w UE, stanowiło wyzwanie. W tym kontekście Komisja wspierała państwa członkowskie w zapewnieniu, aby dostawcy usług hostingowych wywiązywali się z obowiązku wyznaczenia przedstawiciela prawnego w UE oraz zapewnienia punktu kontaktowego (art. 15 ust. 1 rozporządzenia), np. w formie adresu e-mail, w celu zapewnienia, aby działania podejmowano w sposób natychmiastowy. Komisja przypomniała dostawcom usług hostingowych o ich obowiązkach również na różnych forach, w tym na Forum UE ds. Internetu.

Zgodnie z informacjami, którymi dysponuje Komisja, żaden właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych miał główną jednostkę organizacyjną, nie zweryfikował do tej pory nakazu usunięcia na podstawie art. 4 rozporządzenia, aby ustalić, czy nakaz ten nie narusza w sposób poważny lub oczywisty rozporządzenia lub praw podstawowych i wolności, ponieważ dotychczas nie złożono uzasadnionego żądania o dokonanie takiej weryfikacji. W związku z tym do tej pory żaden organ nie stwierdził, aby jakikolwiek nakaz usunięcia naruszył rozporządzenie lub prawa podstawowe w ten sposób.

Dotychczas żaden dostawca usług hostingowych nie przywrócił treści (lub dostępu do nich), które były przedmiotem nakazu usunięcia, na podstawie weryfikacji dokonanej na podstawie art. 4 rozporządzenia, ponieważ taka weryfikacja i takie żądania o przywrócenie nie miały jeszcze miejsca. W związku z tym nie ma informacji na temat tego, jak długo zwykle trwa przywrócenie treści lub dostępu do nich, ani na temat „niezbędnych środków" podjętych przez dostawców usług hostingowych w celu przywrócenia treści lub dostępu do treści.

4.3. ŚRODKI PRAWNE (art. 9)

Zgodnie z informacjami, którymi dysponuje Komisja, dostawcy usług hostingowych do tej pory nie zaskarżyli przed właściwymi sądami nakazów usunięcia ani decyzji wydanych na podstawie

art. 5 ust. 4. Niemniej jednak w przypadku jednego nakazu usunięcia dostawca usług hostingowych twierdził, że wykonanie tego nakazu jest niemożliwe.

Zgodnie z informacjami przekazanymi przez państwa członkowskie[14] co najmniej 12 państw członkowskich posiada „skuteczne procedury" umożliwiające dostawcom usług hostingowych i dostawcom treści zaskarżenie nakazu usunięcia wydanego lub decyzji podjętej na podstawie art. 4 ust. 4 bądź art. 5 ust. 4, 6 lub 7 przed sądami państwa członkowskiego właściwego organu, który wydał dany nakaz usunięcia lub podjął daną decyzję (art. 9 ust. 1 i 2). W państwach członkowskich, w których takie procedury obowiązują, odnoszą się one głównie do postępowań sądowych. Na podstawie aktualnych danych otrzymanych od państw członkowskich nie można jednak stwierdzić, czy procedury te są „skuteczne" czy szczególne dla przedmiotowego rozporządzenia, ponieważ do tej pory nie zaskarżono żadnej decyzji.

4.4. ŚRODKI SZCZEGÓLNE I POWIĄZANE KWESTIE DOTYCZĄCE PRZEJRZYSTOŚCI (art. 5 i 7)

Zgodnie z dostępnymi informacjami żadnego dostawcy usług hostingowych nie uznano dotychczas za narażonego na treści o charakterze terrorystycznym w rozumieniu art. 5 ust. 4 rozporządzenia. W związku z tym wymóg wprowadzenia środków szczególnych określonych w tym artykule nie ma (jeszcze) zastosowania do żadnego dostawcy usług hostingowych.

Należy jednak zauważyć, że zgodnie ze sprawozdaniami z przejrzystości dostarczonymi przez dostawców usług hostingowych część z nich wprowadziła środki w celu przeciwdziałania wykorzystywaniu ich usług do rozpowszechniania treści o charakterze terrorystycznym, w szczególności w drodze przyjęcia szczegółowych warunków umownych oraz stosowania innych przepisów i środków mających na celu ograniczenie rozpowszechniania treści o charakterze terrorystycznym. Jak wskazano powyżej, zgodnie z art. 7 dostawcy usług hostingowych muszą zapewnić przejrzystość w tej kwestii nie tylko w drodze sprawozdawczości w zakresie przejrzystości, ale również przez przedstawienie jasnych informacji w swoich warunkach umownych.

4.5. BEZPOŚREDNIE ZAGROŻENIE ŻYCIA (art. 14 ust. 5)

Art. 14 ust. 5 rozporządzenia stanowi, że w przypadku gdy dostawcy usług hostingowych dowiedzą się o treściach o charakterze terrorystycznym, które wiążą się z bezpośrednim zagrożeniem życia, natychmiast informują organy właściwe w zakresie prowadzenia postępowań przygotowawczych i ścigania przestępstw w zainteresowanym państwie członkowskim lub zainteresowanych państwach członkowskich. Jeżeli nie ma możliwości zidentyfikowania właściwego państwa członkowskiego, dostawca usług hostingowych przekazuje informacje Europolowi na potrzeby odpowiednich dalszych działań.

Do 31 grudnia 2023 r. Komisja otrzymała informacje o dziewięciu przypadkach, w których unijna jednostka ds. zgłaszania podejrzanych treści w internecie działająca w strukturach Europolu

[14] Należy zauważyć, że przekazane informacje mogą nie być kompletne. Uzyskanie całościowego i w pełni aktualnego przeglądu sposobów, przy użyciu których państwa członkowskie wdrożyły wymóg zapewnienia dostępu do skutecznych środków zaskarżenia, wymagałoby przeprowadzenia dalszych ocen.

otrzymała informacje na temat treści o charakterze terrorystycznym, które wiążą się z bezpośrednim zagrożeniem życia. Ponieważ w art. 14 ust. 5 rozporządzenia nie przewidziano obowiązku informowania Europolu we wszystkich przypadkach, liczba powiadomień mogłaby być wyższa. Jedynym państwem członkowskim, które przekazało informacje na temat stosowania art. 14 ust. 5, była Hiszpania. 18 kwietnia 2023 r. organy hiszpańskie otrzymały od platformy Amazon powiadomienie w sprawie domniemanych treści o charakterze terrorystycznym wiążących się z bezpośrednim zagrożeniem życia, które pojawiły się na platformie Twitch poświęconej grom komputerowym. Stwierdzono, że treści te nie spełniają warunków dotyczących treści o charakterze terrorystycznym wiążących się z bezpośrednim zagrożeniem życia w rozumieniu rozporządzenia.

4.6. WSPÓŁPRACA MIĘDZY DOSTAWCAMI USŁUG HOSTINGOWYCH, WŁAŚCIWYMI ORGANAMI ORAZ EUROPOLEM (art. 14)

Jak wspomniano powyżej, aby pomóc państwom członkowskim w wykonywaniu rozporządzenia, Europol opracował platformę o nazwie „PERCI", która centralizuje, koordynuje i ułatwia **przekazywanie nakazów usunięcia i zgłoszeń** do dostawców usług hostingowych. Platforma funkcjonuje od 3 lipca 2023 r. Przed pełnym wdrożeniem PERCI Europol wprowadził rozwiązania awaryjne w celu ułatwienia ręcznego przekazywania nakazów usunięcia, usuwania konfliktów związanych z treścią, aby uniknąć utrudniania toczących się postępowań przygotowawczych, oraz reagowania kryzysowego w sytuacjach „bezpośredniego zagrożenia życia".

PERCI to jednolity system umożliwiający współpracę między właściwymi organami, dostawcami usług hostingowych i Europolem, jak przewidziano w art. 14 rozporządzenia w odniesieniu do kwestii objętych rozporządzeniem. Dokładniej rzecz ujmując, PERCI:

- to oparte na chmurze rozwiązanie opracowane w celu zapewnienia bezpieczeństwa i ochrony danych w chmurze;
- to jednolita platforma współpracy służąca do prowadzenia komunikacji i koordynacji w czasie rzeczywistym, ułatwiająca szybkie usuwanie treści o charakterze terrorystycznym;
- ułatwia weryfikację transgranicznych nakazów usunięcia;
- ułatwia usuwanie konfliktów, co jest istotne, aby uniknąć sytuacji, w której właściwy organ państwa członkowskiego wysyła nakaz usunięcia treści będących przedmiotem trwającego postępowania przygotowawczego w innym państwie członkowskim;
- umożliwia dostawcom usług hostingowych otrzymywanie nakazów usunięcia w sposób jednolity i znormalizowany, za pośrednictwem jednego kanału komunikacyjnego.

PERCI umożliwia również przekazywanie zgłoszeń.

Obecnie oprócz roli, jaką pełni w odniesieniu do zgłoszeń (zob. motyw 40 rozporządzenia), PERCI ułatwia przekazywanie nakazów usunięcia (art. 3 i 4), sprawozdawczość państw członkowskich (art. 8) i koordynację, a także usuwanie konfliktów, gdy toczy się postępowanie przygotowawcze w sprawie treści, wobec których ma zostać wysłany nakaz usunięcia (art. 14).

Obecnie trwają prace nad wykorzystywaniem PERCI do realizacji kolejnych zadań wynikających z rozporządzenia, takich jak weryfikacja transgranicznych nakazów usunięcia (art. 4)[15].

Państwa członkowskie potwierdziły, że zgodnie z art. 14 rozporządzenia:

- właściwe organy wymieniają informacje, koordynują działania i współpracują z innymi właściwymi organami;
- właściwe organy wymieniają informacje, koordynują działania i współpracują z Europolem;
- istnieją mechanizmy mające na celu zacieśnienie współpracy przy jednoczesnym unikaniu konfliktów w zakresie prowadzenia postępowań przygotowawczych prowadzonych w innych państwach członkowskich;
- większość państw członkowskich uznaje PERCI za preferowane narzędzie do przekazywania nakazów usunięcia, ponieważ umożliwia koordynację działań dzięki usuwaniu konfliktów.

4.7. SKUTKI W ZAKRESIE ZGŁOSZEŃ

Zgłoszenia dotyczące treści o charakterze terrorystycznym stanowią dobrowolne narzędzie, z którego korzystano już przed przyjęciem rozporządzenia. Chociaż rozporządzenie nie zawiera szczególnych przepisów dotyczących zgłoszeń, zgodnie z motywem 40 żaden z przepisów rozporządzenia nie uniemożliwia państwom członkowskim i Europolowi wykorzystywania zgłoszeń jako instrumentu służącego do przeciwdziałania treściom o charakterze terrorystycznym w internecie.

Od utworzenia w 2015 r. unijna jednostka ds. zgłaszania podejrzanych treści w internecie działająca w strukturach w Europolu aktywnie identyfikuje treści o charakterze terrorystycznym w internecie i zgłasza je dostawcom usług hostingowych, a także tworzy odpowiednie narzędzia (tj. PERCI, a wcześniej IRMA[16]) ułatwiające przekazywanie zgłoszeń.

Zgodnie z informacjami przekazanymi Komisji organy państw członkowskich nadal korzystają ze zgłoszeń w odniesieniu do niektórych dostawców usług hostingowych, ale mają możliwość

[15] Więcej informacji szczegółowych: – art. 3 i 4: przekazywanie nakazów usunięcia; – art. 3 ust. 6–8: informacje zwrotne od dostawców usług hostingowych; – art. 4 ust. 3–7: mechanizm weryfikacji; – art. 7: sprawozdawczość; – art. 14 ust. 1: usuwanie konfliktów, koordynacja, unikanie powielania wysiłków; – art. 14 ust. 3: bezpieczny kanał komunikacji; – art. 14 ust. 4: korzystanie ze specjalnych narzędzi opracowanych przez Europol; – art. 14 ust. 5: informowanie na temat „bezpośredniego zagrożenia życia”; – motyw 40: przekazywanie zgłoszeń.

[16] Europol opracował aplikację zarządzania zgłoszeniami podejrzanych treści w internecie (IRMA) w 2016 r. na potrzeby zgłaszania nielegalnych treści do dostawców usług internetowych (umieszczania znaczników na tych treściach). Początkowo dostęp do IRMA przyznano pracownikom Europolu i specjalnym jednostkom ds. zgłaszania podejrzanych treści w internecie w siedmiu państwach członkowskich. Aplikację IRMA zastąpiono narzędziem PERCI z dniem 3 lipca 2023 r.

wydania nakazów usunięcia dostawcom usług hostingowych, którzy nie odpowiadają na zgłoszenia, lub z innych powodów, takich jak konieczność pilnego usunięcia treści.

4.8. WSPARCIE NA RZECZ MNIEJSZYCH DOSTAWCÓW USŁUG HOSTINGOWYCH W CELU WYKONYWANIA ROZPORZĄDZENIA

W rozporządzeniu nałożono na dostawców usług hostingowych szereg obowiązków. Podczas gdy duzi dostawcy usług hostingowych zazwyczaj dysponują zdolnościami technicznymi, odpowiednim personelem weryfikacyjnym i wiedzą fachową potrzebnymi do wykonywania rozporządzenia, małe podmioty mogą posiadać mniejsze zasoby finansowe, techniczne i ludzkie oraz wiedzę fachową w tym zakresie. Jednocześnie mniejsi dostawcy usług hostingowych są coraz częściej ofiarami ataków mających na celu wykorzystanie ich usług. Można to również przypisać skutecznym wysiłkom w zakresie moderowania treści podejmowanym przez większych dostawców usług hostingowych. Chociaż tendencja ta pokazuje, że moderowanie treści jest skuteczne, wynika z niej również konieczność wspierania mniejszych dostawców usług hostingowych w zwiększaniu ich zdolności i wiedzy pod kątem spełniania wymogów rozporządzenia.

Aby sprostać temu wyzwaniu, Komisja ogłosiła zaproszenie do składania wniosków w ramach Funduszu Bezpieczeństwa Wewnętrznego, aby wesprzeć mniejszych dostawców usług hostingowych w wykonywaniu rozporządzenia[17]. Komisja wybrała trzy projekty[18], aby wesprzeć ich na trzy sposoby. Po pierwsze, w drodze informowania i zwiększania świadomości na temat przepisów i wymogów rozporządzenia, po drugie, w drodze opracowania, wdrożenia i uruchomienia narzędzi i mechanizmów niezbędnych do przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, a po trzecie, w drodze wymiany doświadczeń i najlepszych praktyk w całym sektorze.

W 2023 r. rozpoczęto realizację tych trzech projektów i przyniosły one już wartościowe rezultaty. Na przykład w sprawozdaniu z identyfikacji i grupowania w ramach projektu FRISCO[19] ustalono, że mikro- i mali dostawcy usług hostingowych zazwyczaj posiadają bardzo ograniczoną wiedzę na temat rozporządzenia, oraz wskazano potencjalne trudności, jakie mogą oni napotkać w wykonywaniu nakazów usunięcia w ciągu jednej godziny, ponieważ często nie dysponują obsługą całodobową. Problemem jest brak zasobów, a także nawiązanie kanałów komunikacji z organami ścigania. Ponad połowa dostawców usług hostingowych zbadanych w ramach projektu nie moderuje treści wytwarzanych przez użytkowników i oznajmiła, że nigdy nie napotkała na

[17] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/isf/wp-call/2021-2022/call-fiche_isf-2021-ag-tco_en.pdf

[18] 1) Oparte na AI ramy wsparcia dla mikro (i małych) dostawców usług hostingowych w zakresie zgłaszania i usuwania treści terrorystycznych w internecie (ALLIES), 2) zwalczanie treści terrorystycznych w internecie (FRISCO) i 3) technologia przeciwko terroryzmowi w Europie (TATE). Więcej informacji pod następującym adresem: Finansowanie i przetargi (europa.eu).

[19] Obejmuje to okres sześciomiesięczny, który zakończył się w maju 2023 r. Sprawozdanie sporządzono na podstawie informacji zwrotnej otrzymanej od 48 europejskich dostawców usług hostingowych, z których 33 udzieliło odpowiedzi za pośrednictwem kwestionariusza internetowego, a 15 podczas wywiadów. FRISCO, *D2.1: Sprawozdanie z identyfikacji i grupowania potrzeb i barier w zakresie zgodności: zrozumienie potrzeb małych i mikro dostawców usług hostingowych w odniesieniu do wypełniania wymogów rozporządzenia w sprawie treści o charakterze terrorystycznym w internecie oraz świadomości tych dostawców w tej dziedzinie;* dokument dostępny pod adresem: Deliverables | Frisco (friscoproject.eu).

swoich platformach treści o charakterze terrorystycznym. Jeżeli takie treści pojawią się na ich platformach, tacy dostawcy usług hostingowych prawdopodobnie zastosują środki doraźne.

W ramach tych trzech projektów mali dostawcy usług hostingowych otrzymują wsparcie w dążeniu do przestrzegania przepisów rozporządzenia, również w drodze tworzenia punktów kontaktowych i wdrażania mechanizmów rozpatrywania skarg użytkowników.

Również art. 3 ust. 2 rozporządzenia – który wymaga terminowego przekazywania informacji na temat mających zastosowanie procedur i terminów dostawcom usług hostingowych, wobec których nie wydano wcześniej nakazu usunięcia – może mieć znaczenie w szczególności dla mniejszych dostawców usług hostingowych.

4.9. GWARANCJE W ZAKRESIE OCHRONY PRAW PODSTAWOWYCH

Rozporządzenie zawiera różne zabezpieczenia mające na celu zwiększenie rozliczalności i przejrzystości w odniesieniu do usuwania treści o charakterze terrorystycznym z internetu. W tym względzie należy się odnieść do wcześniejszych sekcji, w szczególności do przedstawionych informacji na temat środków prawnych, sprawozdawczości i specjalnego mechanizmu dotyczącego transgranicznych nakazów usunięcia.

Ponadto w art. 23 rozporządzenia zobowiązano Komisję do składania sprawozdań ze skuteczności funkcjonowania mechanizmów gwarancyjnych i zabezpieczających, w szczególności tych przewidzianych w art. 4 ust. 4, art. 6 ust. 3 i art. 7–11, w kontekście oceny rozporządzenia. Takie gwarancje dotyczą skarg, środków prawnych i mechanizmów w zakresie kar przyjętych i wdrożonych, aby – w celu ochrony dostawców treści i dostawców usług hostingowych – uniknąć ryzyka usunięcia z internetu treści błędnie uznanych za treści o charakterze terrorystycznym. Ocena funkcjonowania i skuteczności mechanizmów ochronnych będzie zatem częścią oceny na podstawie art. 23.

W tym względzie w programie monitorowania, o którym mowa w art. 21 ust. 2 rozporządzenia, określono system wskaźników na potrzeby oceny wpływu rozporządzenia na prawa podstawowe, które to wskaźniki zostaną uwzględnione w ocenie rozporządzenia.

Program monitorowania zostanie wykorzystany do sporządzenia oceny funkcjonowania i skuteczności mechanizmów gwarancyjnych i zabezpieczających wdrożonych w kontekście rozporządzenia oraz ich wpływu na prawa podstawowe, która zostanie przeprowadzona w ramach oceny rozporządzenia. Ten zakres oddziaływań obejmuje dwa obszary wymienione w art. 23 rozporządzenia: a) skuteczność funkcjonowania mechanizmów gwarancyjnych i zabezpieczających, w szczególności tych przewidzianych w art. 4 ust. 4, art. 6 ust. 3 i art. 7–11; b) wpływ stosowania przedmiotowego rozporządzenia na prawa podstawowe, w szczególności na wolność wypowiedzi i informacji, poszanowanie życia prywatnego i ochronę danych osobowych.

4.10. WŁAŚCIWE ORGANY (art. 13)

Art. 13 rozporządzenia stanowi, że państwa członkowskie muszą zapewnić, aby ich właściwe organy dysponowały niezbędnymi uprawnieniami i wystarczającymi zasobami, aby osiągnąć cele

i wypełnić swoje obowiązki określone w rozporządzeniu. Niektóre państwa członkowskie wdrożyły następujące środki służące zapewnieniu, aby właściwe organy dysponowały niezbędnymi uprawnieniami i wystarczającymi zasobami:

- ustanowienie nowych organów/dyrekcji;
- przydzielenie dodatkowych funduszy i dodatkowego personelu;
- utworzenie nowych ram prawnych.

5. WNIOSKI

Niezwykle ważne jest pełne wdrożenie wszystkich narzędzi i środków na szczeblu UE w celu szybkiego zwalczania nielegalnych treści rozpowszechnianych w internecie. Ma to znaczenie szczególnie ze względu na samą skalę takich nielegalnych treści, o czym świadczą ostatnio rozpowszechnianie treści związane z atakiem przeprowadzonym przez Hamas na Izrael.

Rozporządzenie przyczynia się do zwiększenia bezpieczeństwa publicznego w całej Unii celem zapobiegania wykorzystywaniu dostawców usług hostingowych działających na rynku wewnętrznym przez terrorystów do szerzenia ich przesłania w celu zastraszenia, radykalizacji, rekrutacji i ułatwiania ataków terrorystycznych.

W następstwie wszczęcia w styczniu 2023 r. postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego **osiągnięto pewne postępy**. Do 31 grudnia 2023 r. 23 państwa członkowskie wyznaczyły właściwe organy na podstawie art. 12 ust. 1, co odzwierciedlają informacje opublikowane w rejestrze internetowym, i w rezultacie zaczęto bardziej systematycznie stosować środki i narzędzia przewidziane w rozporządzeniu. Ponadto do 21 grudnia 2023 r. zamknięto 11 z 22 postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego wszczętych w styczniu 2023 r. Komisja wzywa pozostałe państwa członkowskie do podjęcia niezbędnych kroków w celu wyznaczenia właściwych organów na podstawie art. 12 ust. 1 i wypełnienia obowiązków wynikających z art. 12 ust. 2, art. 12 ust. 3 i art. 18 ust. 1.

Ogólnie rzecz biorąc, państwa członkowskie zgłosiły, że przekazywanie nakazów usunięcia dostawcom usług hostingowych przy wsparciu Europolu przebiega sprawnie. Z informacji otrzymanych od państw członkowskich i Europolu wynika, że od momentu rozpoczęcia stosowania rozporządzenia przekazano co najmniej 349 **nakazów usunięcia treści o charakterze terrorystycznym**. W dziesięciu przypadkach jeden dostawca usług hostingowych nie usunął treści o charakterze terrorystycznym lub nie zablokował dostępu do nich w maksymalnym terminie jednej godziny określonym w rozporządzeniu.

Z informacji otrzymanych od państw członkowskich i Europolu wynika, że chociaż rozporządzenie nie zawiera żadnych przepisów w zakresie zgłoszeń, od czasu wejścia rozporządzenia w życie wzrosła szybkość reagowania na zgłoszenia dotyczące treści o charakterze terrorystycznym. Ponadto w dziewięciu przypadkach Europol otrzymał od dostawców usług hostingowych informacje na temat treści o charakterze terrorystycznym, które wiążą się z bezpośrednim zagrożeniem życia, zgodnie z art. 14 ust. 5.

Funkcjonują skuteczniejsze kanały komunikacyjne i procedury w zakresie komunikacji, w szczególności od momentu uruchomienia platformy PERCI w dniu 3 lipca 2023 r., co doprowadziło do przekazywania nakazów usunięcia w sposób bardziej systematyczny, przy czym narzędzie to służy również do przekazywania dużej liczby zgłoszeń. Państwa członkowskie i Europol spodziewają się, że uruchomienie PERCI ułatwi wykorzystywanie tych instrumentów do zwalczania treści o charakterze terrorystycznym w internecie.

Na tej podstawie Komisja stwierdza, że, ogólnie rzecz biorąc, rozporządzenie miało **pozytywny wpływ** na ograniczenie rozpowszechniania w internecie treści o charakterze terrorystycznym. Niemniej jednak w dziesięciu przypadkach na 349 dostawca usług hostingowych przekroczył ustanowiony w rozporządzeniu maksymalny jednogodzinny termin usunięcia treści o charakterze terrorystycznym lub zablokowania dostępu do nich.

Komisja aktywnie wspiera państwa członkowskie i dostawców usług hostingowych, w tym w formie warsztatów technicznych organizowanych przed rozpoczęciem stosowania rozporządzenia i po tym terminie. Ostatnie takie warsztaty odbyły się 24 listopada 2023 r. Komisja wspiera również mniejszych dostawców usług hostingowych, aby szybko zapewnić pełne stosowanie rozporządzenia oraz pomóc im w radzeniu sobie z dotychczas napotkanymi wyzwaniami.

Komisja będzie w dalszym ciągu nadzorowała wykonanie przepisów przedmiotowego rozporządzenia i ich stosowanie. Komisja będzie ściśle monitorować skuteczność instrumentów przewidzianych w rozporządzeniu za pośrednictwem programu monitorowania, który zostanie uwzględniony w ocenie rozporządzenia przeprowadzonej na podstawie art. 23.