KOMISJA
EUROPEJSKA

Bruksela, dnia 12.9.2018 r.
COM(2018) 640 final

2018/0331 (COD)

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.

{SEC(2018) 397 final} - {SWD(2018) 408 final} - {SWD(2018) 409 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

1.1. Przyczyny i cele wniosku

Wszechobecność internetu umożliwia jego użytkownikom komunikowanie się, pracę, kontakty towarzyskie, tworzenie, uzyskiwanie i wymianę informacji i treści z setkami milionów ludzi na całym świecie. Platformy internetowe przynoszą znaczące korzyści dla dobrobytu ekonomicznego i społecznego użytkowników w całej Unii i poza nią. Jednak możliwość dotarcia do tak dużej grupy odbiorców przy minimalnych kosztach przyciąga również przestępców, którzy chcą korzystać z internetu do celów niezgodnych z prawem. Niedawne ataki terrorystyczne na terenie UE pokazały, w jaki sposób terroryści wykorzystują internet do pozyskiwania zwolenników, przygotowywania i ułatwiania działalności terrorystycznej, do gloryfikowania swojego okrucieństwa, nakłaniania innych do pójścia w ich ślady i szerzenia strachu w społeczeństwie.

Treści o charakterze terrorystycznym przekazywane w internecie do takich celów są rozpowszechniane za pośrednictwem dostawców usług hostingowych, którzy umożliwiają przesyłanie treści dostarczonych przez osoby trzecie. Treści o charakterze terrorystycznym w internecie okazały się decydujące przy radykalizacji i inspirowaniu ataków tzw. „samotnych wilków" w przypadku kilku niedawnych ataków terrorystycznych w Europie. Treści takie nie tylko powodują znaczne negatywne skutki dla osób fizycznych i ogółu społeczeństwa, ale również ograniczają zaufanie użytkowników do internetu i wpływają na modele biznesowe oraz reputację dotkniętych przedsiębiorstw. Terroryści wykorzystują do tego celu nie tylko duże platformy mediów społecznościowych, ale również coraz częściej mniejszych dostawców oferujących różne rodzaje usług hostingowych na całym świecie. Takie niewłaściwe wykorzystanie internetu uwydatnia szczególną odpowiedzialność społeczną platform internetowych w zakresie ochrony użytkowników przed narażeniem na treści o charakterze terrorystycznym oraz poważne zagrożenia bezpieczeństwa, jakie niosą ze sobą te treści dla całego społeczeństwa.

Dostawcy usług hostingowych, odpowiadając na wezwania organów publicznych, wprowadzili pewne środki w celu rozwiązania problemu treści o charakterze terrorystycznym w swoich usługach. Poczyniono postępy poprzez dobrowolne struktury i partnerstwa, w tym Forum UE ds. Internetu, które zostało zainicjowane w grudniu 2015 r. w ramach Europejskiej agendy bezpieczeństwa. W ramach Forum UE ds. Internetu promowano dobrowolną współpracę i działania państw członkowskich i dostawców usług hostingowych mające na celu ograniczenie dostępu do treści o charakterze terrorystycznym w internecie oraz wzmocnienie pozycji społeczeństwa obywatelskiego przy zwiększaniu ilości skutecznych alternatywnych treści w internecie. Wysiłki te przyczyniły się do zacieśnienia współpracy, poprawy reakcji przedsiębiorstw na zgłoszenia organów krajowych i jednostki Europolu ds. zgłaszania podejrzanych treści w internecie, wdrożenia dobrowolnych proaktywnych środków w celu poprawy zautomatyzowanego wykrywania treści o charakterze terrorystycznym, zacieśnienia współpracy w ramach sektora – w tym opracowania „bazy hashów", aby zapobiec umieszczaniu znanych treści o charakterze terrorystycznym na powiązanych platformach – jak również zwiększonej przejrzystości działań. Podczas gdy współpraca w ramach Forum UE ds. Internetu powinna być kontynuowana w przyszłości, okazało się, że dobrowolne ustalenia mają również swoje ograniczenia. Po pierwsze nie wszyscy zainteresowani dostawcy usług hostingowych uczestniczyli w Forum, a po drugie, ogólna skala i tempo postępu wśród dostawców usług hostingowych nie są wystarczające, aby właściwie rozwiązać ten problem.

Biorąc pod uwagę te ograniczenia, istnieje wyraźna potrzeba zintensyfikowania działań Unii Europejskiej w zakresie zwalczania treści o charakterze terrorystycznym w internecie. W dniu 1 marca 2018 r. Komisja przyjęła zalecenie w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie, opierając się na komunikacie Komisji z września[1] oraz na działaniach prowadzonych w ramach Forum UE ds. Internetu. W zaleceniu zawarto specjalny rozdział określający szereg środków mających skutecznie powstrzymać zamieszczanie i rozpowszechnianie propagandy terrorystycznej w internecie, takich jak ulepszenia procesu przekazywania zgłoszeń, godzinny termin na zareagowanie na zgłoszenie, bardziej aktywne wykrywanie, skuteczne usuwanie i wystarczające gwarancje służące dokładnej ocenie treści o charakterze terrorystycznym[2].

Potrzeba intensyfikacji działań w związku z treściami o charakterze terrorystycznym w internecie została również potwierdzona przez państwa członkowskie UE, a niektóre z nich uchwaliły już odpowiednie przepisy lub wyraziły taki zamiar. W następstwie szeregu ataków terrorystycznych w UE oraz biorąc pod uwagę fakt, że treści o charakterze terrorystycznym są w dalszym ciągu łatwo dostępne, podczas posiedzenia w dniach 22–23 czerwca 2017 r. Rada Europejska wezwała branżę do opracowania nowych technologii i narzędzi usprawniających „automatyczne wykrywanie treści podżegających do aktów terrorystycznych i usuwanie tych treści. W razie konieczności należy to uzupełnić odpowiednimi środkami ustawodawczymi na szczeblu UE". W dniu 28 czerwca 2018 r. Rada Europejska z zadowoleniem przyjęła „zamiar przedstawienia przez Komisję wniosku ustawodawczego służącego poprawie wykrywania i usuwania treści podżegających do nienawiści i do działań terrorystycznych". Ponadto Parlament Europejski w swojej rezolucji w sprawie platform internetowych i jednolitego rynku cyfrowego z dnia 15 czerwca 2017 r. wezwał te platformy „do wzmocnienia środków zwalczania nielegalnych i szkodliwych treści" oraz wezwał Komisję do przedstawienia wniosków w celu rozwiązania tych problemów.

Aby sprostać tym wyzwaniom i w odpowiedzi na wezwania państw członkowskich i Parlamentu Europejskiego, celem niniejszego wniosku Komisji jest ustanowienie jasnych i zharmonizowanych ram prawnych na potrzeby zapobiegania wykorzystywaniu usług hostingowych do rozpowszechniania w internecie treści o charakterze terrorystycznym, aby zagwarantować sprawne funkcjonowanie jednolitego rynku cyfrowego, przy jednoczesnym zapewnieniu zaufania i bezpieczeństwa. Niniejsze rozporządzenie ma na celu zapewnienie jasności co do odpowiedzialności dostawców usług hostingowych za podejmowanie wszelkich stosownych, rozsądnych i proporcjonalnych działań niezbędnych do zapewnienia bezpieczeństwa świadczonych przez nich usług oraz do sprawnego i skutecznego wykrywania i usuwania treści o charakterze terrorystycznym w internecie, z uwzględnieniem podstawowego znaczenia wolności wypowiedzi i informacji w ramach otwartego i demokratycznego społeczeństwa. Wprowadza ono również szereg niezbędnych gwarancji, których celem jest zapewnienie pełnego poszanowania praw podstawowych, takich jak wolność wypowiedzi i informacji w demokratycznym społeczeństwie, oprócz sądowych środków odwoławczych zagwarantowanych przez prawo do skutecznego środka odwoławczego, o którym mowa w art. 19 TUE i art. 47 Karty praw podstawowych Unii Europejskiej.

Nakładając minimalny zestaw obowiązków w zakresie staranności na podmioty świadczące usługi hostingowe, który obejmuje pewne szczegółowe zasady i obowiązki, oraz nakładając

[1] Komunikat (COM(2017) 555 final) w sprawie zwalczania nielegalnych treści w internecie.

[2] Zalecenie (C(2018) 1177 final) z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie.

obowiązki na państwa członkowskie, niniejszy wniosek ma na celu zwiększenie skuteczności obecnych środków w zakresie wykrywania, identyfikacji i usuwania treści o charakterze terrorystycznym w internecie, bez naruszania praw podstawowych, takich jak wolność wypowiedzi i informacji. Takie zharmonizowane ramy prawne ułatwią świadczenie usług online na całym jednolitym rynku cyfrowym, zapewnią równe warunki działania wszystkim dostawcom usług hostingowych kierującym swoje usługi do Unii Europejskiej oraz zapewnią solidne ramy prawne dla wykrywania i usuwania treści o charakterze terrorystycznym, którym towarzyszyć będą odpowiednie zabezpieczenia w celu ochrony praw podstawowych. W szczególności obowiązki w zakresie przejrzystości zwiększą zaufanie obywateli, a zwłaszcza użytkowników internetu, oraz odpowiedzialność i przejrzystość działań przedsiębiorstw, w tym wobec organów publicznych. We wniosku określono również obowiązki w zakresie wprowadzenia środków naprawczych i mechanizmów rozpatrywania skarg w celu zapewnienia użytkownikom możliwości zakwestionowania usunięcia ich treści. Obowiązki państw członkowskich przyczynią się do osiągnięcia tych celów, a także poprawią możliwości właściwych organów w zakresie podejmowania odpowiednich działań przeciwko treściom o charakterze terrorystycznym w internecie oraz w zakresie zwalczania przestępczości. W przypadku nieprzestrzegania rozporządzenia przez dostawców usług hostingowych państwa członkowskie mogą nałożyć sankcje.

1.2. Spójność z unijnymi ramami prawnymi obowiązującymi w tej dziedzinie polityki

Niniejszy wniosek jest zgodny z dorobkiem prawnym w dziedzinie jednolitego rynku cyfrowego, a w szczególności z dyrektywą o handlu elektronicznym. W szczególności wszelkie środki wprowadzane przez dostawcę usług hostingowych zgodnie z niniejszym rozporządzeniem, w tym wszelkie proaktywne środki, nie powinny same w sobie prowadzić do utraty przez dostawcę usług korzyści polegającej na zwolnieniu od odpowiedzialności, przewidzianym, na określonych warunkach, w art. 14 dyrektywy o handlu elektronicznym. Podjęcie przez organy krajowe decyzji o narzuceniu proporcjonalnych i szczególnych proaktywnych środków nie powinno co do zasady prowadzić do nałożenia na państwa członkowskie ogólnego obowiązku monitorowania, określonego w art. 15 ust. 1 dyrektywy 2000/31/WE. Biorąc jednak pod uwagę szczególnie poważne zagrożenia związane z rozpowszechnianiem treści o charakterze terrorystycznym, decyzje podjęte na mocy niniejszego rozporządzenia mogą wyjątkowo stanowić odstępstwo od tej zasady w ramach UE. Przed przyjęciem takich decyzji właściwy organ powinien zachować równowagę między potrzebami w zakresie bezpieczeństwa publicznego a odnośnymi interesami i prawami podstawowymi, w tym w szczególności wolnością wypowiedzi i informacji, wolnością prowadzenia działalności gospodarczej, ochroną danych osobowych i prywatności. Obowiązki dochowania staranności przez dostawców usług hostingowych powinny odzwierciedlać i uwzględniać tę równowagę, co zostało wyrażone w dyrektywie o handlu elektronicznym.

Wniosek jest również spójny i ściśle powiązany z dyrektywą (UE) 2017/541 w sprawie zwalczania terroryzmu, której celem jest harmonizacja prawodawstw państw członkowskich w zakresie kryminalizacji przestępstw terrorystycznych. Art. 21 dyrektywy w sprawie zwalczania terroryzmu zobowiązuje państwa członkowskie do przyjmowania środków zapewniających natychmiastowe usuwanie treści internetowych publicznie nawołujących do popełnienia przestępstwa terrorystycznego i pozostawia państwom członkowskim wybór takich środków. Niniejsze rozporządzenie, ze względu na swój prewencyjny charakter, obejmuje nie tylko materiały podżegające do terroryzmu, ale także materiały do celów rekrutacji lub szkolenia, odzwierciedlając inne przestępstwa związane z działalnością terrorystyczną, które również wchodzą w zakres dyrektywy (UE) 2017/541. Niniejsze

rozporządzenie bezpośrednio nakłada obowiązki w zakresie staranności na dostawców usług hostingowych w odniesieniu do usuwania treści o charakterze terrorystycznym i harmonizuje procedury dotyczące nakazów usunięcia w celu ograniczenia dostępności treści o charakterze terrorystycznym w internecie.

Rozporządzenie to uzupełnia przepisy określone w przyszłej dyrektywie o audiowizualnych usługach medialnych, ponieważ jego zakres podmiotowy i przedmiotowy są szersze. Rozporządzenie obejmuje nie tylko platformy udostępniania plików wideo, ale wszystkich dostawców usług hostingowych. Ponadto obejmuje ono nie tylko nagrania wideo, ale także obrazy i tekst. Ponadto niniejsze rozporządzenie wykracza poza dyrektywę pod względem przepisów prawa materialnego, ponieważ harmonizuje przepisy dotyczące wniosków o usunięcie treści o charakterze terrorystycznym oraz proaktywnych środków.

Rozporządzenie, którego dotyczy wniosek, opiera się na zaleceniu Komisji z marca 2018 r.[3] w sprawie nielegalnych treści. Zalecenie to nadal obowiązuje, a wszystkie osoby, które mają do odegrania rolę w ograniczaniu dostępu do nielegalnych treści – w tym treści o charakterze terrorystycznym – powinny nadal dostosowywać swoje wysiłki do środków określonych w zaleceniu.

1.3. Krótki opis proponowanego rozporządzenia

Zakres podmiotowy wniosku obejmuje dostawców usług hostingowych, którzy oferują swoje usługi w Unii, niezależnie od ich miejsca prowadzenia działalności czy ich wielkości. Proponowane prawo wprowadza szereg środków mających na celu zapobieganie wykorzystywaniu usług hostingowych do rozpowszechniania w internecie treści o charakterze terrorystycznym w celu zagwarantowania sprawnego funkcjonowania jednolitego rynku cyfrowego, przy jednoczesnym zapewnieniu zaufania i bezpieczeństwa. Definicja nielegalnych treści o charakterze terrorystycznym jest zgodna z definicją przestępstw terrorystycznych określoną w dyrektywie (UE) 2017/541 i jest określona jako informacje, które są wykorzystywane do podżegania do popełniania przestępstw terrorystycznych i ich gloryfikacji, zachęcania do wnoszenia wkładu do nich oraz dostarczania instrukcji dotyczących popełniania przestępstw terrorystycznych, a także promowania uczestnictwa w grupach terrorystycznych.

Aby zapewnić usunięcie nielegalnych treści o charakterze terrorystycznym, rozporządzenie wprowadza nakaz usunięcia, który może zostać wydany jako decyzja administracyjna lub orzeczenie sądowe przez właściwy organ w państwie członkowskim. W takich przypadkach dostawca usług hostingowych jest zobowiązany do usunięcia danych treści lub uniemożliwienia dostępu do nich w ciągu jednej godziny. Ponadto w rozporządzeniu dokonano harmonizacji minimalnych wymogów dotyczących zgłoszeń przesyłanych przez właściwe organy państw członkowskich oraz przez organy Unii (takie jak Europol) dostawcom usług hostingowych, które mają zostać poddane ocenie w świetle odpowiednich warunków ustanowionych przez dostawców usług hostingowych. Wreszcie rozporządzenie nakłada na dostawców usług hostingowych wymóg, aby w stosownych przypadkach wprowadzali proaktywne środki proporcjonalne do poziomu zagrożenia oraz aby usuwali materiały o charakterze terrorystycznym ze swoich usług, w tym za pomocą automatycznych narzędzi do wykrywania.

Środkom mającym na celu ograniczenie treści o charakterze terrorystycznym w internecie towarzyszy szereg kluczowych gwarancji zapewniających pełną ochronę praw

[3] Zalecenie (C(2018) 1177 final) z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie.

podstawowych. W ramach środków mających na celu ochronę treści, które nie stanowią treści o charakterze terrorystycznym, przed omyłkowym usunięciem, we wniosku określono obowiązki dotyczące wprowadzenia środków naprawczych i mechanizmy rozpatrywania skarg, aby zapewnić użytkownikom możliwość zakwestionowania usunięcia ich treści. Ponadto rozporządzenie wprowadza obowiązek przejrzystości w odniesieniu do środków wprowadzanych w celu zwalczania treści o charakterze terrorystycznym przez dostawców usług hostingowych, zapewniając w ten sposób odpowiedzialność wobec użytkowników, obywateli i organów publicznych.

Rozporządzenie nakłada również na państwa członkowskie obowiązek zapewnienia, aby ich właściwe organy miały niezbędną zdolność do interwencji w odniesieniu do treści o charakterze terrorystycznym w internecie. Ponadto państwa członkowskie są zobowiązane do informowania się i wzajemnej współpracy oraz mogą korzystać z kanałów ustanowionych przez Europol w celu zapewnienia koordynacji w odniesieniu do nakazów usunięcia i zgłoszeń. Rozporządzenie przewiduje również obowiązek dla dostawców usług hostingowych polegający na składaniu bardziej szczegółowych sprawozdań na temat wprowadzonych środków i informowaniu organów ścigania, gdy wykryją treści stanowiące zagrożenie dla życia lub bezpieczeństwa. Ponadto na dostawcach usług hostingowych spoczywa obowiązek zachowania usuwanych treści, co stanowi gwarancję na wypadek błędnego usunięcia i zapewnia zachowanie potencjalnych dowodów na potrzeby zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

2.1. Podstawa prawna

Podstawę prawną stanowi art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, który przewiduje ustanowienie środków w celu zapewnienia funkcjonowania rynku wewnętrznego.

Art. 114 stanowi odpowiednią podstawę prawną dla zharmonizowania warunków, na jakich dostawcy usług hostingowych świadczą usługi transgraniczne na jednolitym rynku cyfrowym, a także dla zniwelowania różnic między przepisami poszczególnych państw członkowskich, które w przeciwnym razie mogłyby utrudniać funkcjonowanie rynku wewnętrznego. Zapobiega również pojawianiu się w przyszłości przeszkód dla działalności gospodarczej wynikających z różnic w sposobie rozwoju prawa krajowego.

Art. 114 TFUE może również zostać wykorzystany do nałożenia obowiązków na dostawców usług mających miejsce prowadzenia działalności poza terytorium UE, w przypadku gdy świadczenie przez nich usług ma wpływ na rynek wewnętrzny, ponieważ jest to niezbędne do osiągnięcia pożądanego celu na rynku wewnętrznym.

2.2. Wybór instrumentu

Art. 114 TFUE daje unijnym ustawodawcom możliwość przyjmowania rozporządzeń i dyrektyw.

Ponieważ wniosek dotyczy obowiązków nałożonych na dostawców usług, którzy zazwyczaj oferują swoje usługi w więcej niż jednym państwie członkowskim, rozbieżność w stosowaniu tych przepisów utrudniłaby świadczenie usług przez dostawców usług prowadzących działalność w kilku państwach członkowskich. Rozporządzenie pozwala na nałożenie takiego samego obowiązku w jednolity sposób w całej Unii, jest bezpośrednio stosowane, zapewnia jasność i większą pewność prawa oraz zapobiega rozbieżnej transpozycji w państwach

członkowskich. Z tych powodów najbardziej odpowiednią formą, którą należy zastosować dla tego instrumentu, jest rozporządzenie.

2.3. Pomocniczość

Ze względu na transgraniczny wymiar poruszanych tutaj problemów środki uwzględnione we wniosku muszą zostać przyjęte na szczeblu unijnym, aby osiągnąć cele rozporządzenia. Internet ma ze swej natury charakter transgraniczny, a treść dostępna w jednym państwie członkowskim jest zazwyczaj dostępna z każdego innego państwa członkowskiego.

Pojawiają się rozdrobnione ramy krajowych przepisów w zakresie zwalczania treści o charakterze terrorystycznym w internecie, a ryzyko rośnie. Doprowadziłoby to do obciążenia przedsiębiorstw, które byłyby zmuszone do przestrzegania rozbieżnych przepisów, i stworzyłoby nierówne warunki dla przedsiębiorstw oraz luki w dziedzinie bezpieczeństwa.

Działania UE wzmacniają zatem pewność prawa i zwiększają skuteczność działań podejmowanych przez dostawców usług hostingowych w odniesieniu do treści o charakterze terrorystycznym w internecie. Powinno to umożliwić większej liczbie przedsiębiorstw, w tym przedsiębiorstw mających miejsce prowadzenia działalności poza Unią Europejską, podejmowanie działań, co wzmocni integralność jednolitego rynku cyfrowego.

Uzasadnia to konieczność podjęcia działań przez UE, wyrażoną w konkluzjach Rady Europejskiej z czerwca 2018 r., w których zwrócono się do Komisji o przedstawienie wniosku ustawodawczego w tym obszarze.

2.4. Proporcjonalność

We wniosku określono przepisy, zgodnie z którymi dostawcy usług hostingowych muszą stosować środki w celu szybkiego usuwania treści o charakterze terrorystycznym ze swoich usług. Kluczowe elementy ograniczają wniosek do tego, co jest konieczne do osiągnięcia celów polityki.

Wniosek uwzględnia obciążenie dostawców usług hostingowych i gwarancje, w tym ochronę wolności wypowiedzi i informacji, jak również innych praw podstawowych. Godzinny termin usunięcia ma zastosowanie wyłącznie do nakazów usunięcia, w odniesieniu do których właściwe organy stwierdziły niezgodność z prawem w decyzji, która podlega zaskarżeniu na drodze sądowej. W przypadku zgłoszeń istnieje obowiązek wprowadzenia środków mających na celu ułatwienie szybkiej oceny treści o charakterze terrorystycznym, bez nakładania jednak ani obowiązku ich usunięcia, ani bezwzględnych terminów. Ostateczna decyzja pozostaje w gestii dostawcy usług hostingowych. Obciążenie przedsiębiorstw związane z oceną treści zostaje zmniejszone przez fakt, że właściwe organy państw członkowskich oraz organy Unii przedstawiają wyjaśnienia, dlaczego treści te można uznać za treści o charakterze terrorystycznym. W stosownych przypadkach dostawcy usług hostingowych wprowadzają proaktywne środki w celu ochrony swoich usług przed rozpowszechnianiem treści o charakterze terrorystycznym. Szczególne obowiązki określone w odniesieniu do proaktywnych środków ograniczają się do dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, co potwierdza otrzymanie nakazu usunięcia, który stał się prawomocny, i powinny być proporcjonalne do poziomu zagrożenia oraz zasobów przedsiębiorstwa. Zachowanie usuniętych treści i związanych z nimi danych jest ograniczone czasowo, proporcjonalnie do celów administracyjnego lub sądowego postępowania odwoławczego oraz do celu zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania.

3. WYNIKI OCEN *EX POST*, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

3.1. Konsultacje z zainteresowanymi stronami

Przygotowując niniejszy wniosek ustawodawczy, Komisja przeprowadziła konsultacje ze wszystkimi zainteresowanymi stronami w celu zrozumienia ich opinii i możliwego kierunku działania. Komisja przeprowadziła otwarte konsultacje publiczne w sprawie środków mających na celu poprawę skuteczności zwalczania nielegalnych treści, w ramach których otrzymano 8 961 odpowiedzi, z których 8 749 pochodziło od osób indywidualnych, 172 od organizacji, 10 od organów administracji publicznej, a 30 od innych kategorii respondentów. Równolegle przeprowadzono badanie Eurobarometr z losową próbą 33 500 mieszkańców UE na temat nielegalnych treści w internecie. W maju i czerwcu 2018 r. Komisja przeprowadziła również konsultacje z organami państw członkowskich oraz dostawcami usług hostingowych na temat szczególnych środków mających na celu zwalczanie treści o charakterze terrorystycznym w internecie.

Większość zainteresowanych stron wyraziła opinię, że treści o charakterze terrorystycznym w internecie stanowią poważny problem społeczny, który dotyczy użytkowników internetu i modeli biznesowych dostawców usług hostingowych. Ogólniej rzecz biorąc, 65 % respondentów uczestniczących w badaniu Eurobarometr[4] uznało, że internet nie jest bezpieczny dla użytkowników, a 90 % respondentów uważa, że ważne jest ograniczenie rozpowszechniania nielegalnych treści w internecie. Konsultacje z państwami członkowskimi ujawniły, że chociaż dobrowolne ustalenia przynoszą rezultaty, wiele państw członkowskich postrzega potrzebę wprowadzenia wiążących zobowiązań w odniesieniu do treści o charakterze terrorystycznym, co znalazło odzwierciedlenie w konkluzjach Rady Europejskiej z czerwca 2018 r. Chociaż ogólnie rzecz biorąc, dostawcy usług hostingowych opowiedzieli się za utrzymaniem środków dobrowolnych, odnotowali możliwe negatywne skutki pojawiającego się rozdrobnienia prawnego w Unii.

Wiele zainteresowanych stron zwróciło również uwagę na potrzebę zapewnienia, aby wszelkie środki regulacyjne dotyczące usuwania treści, w szczególności proaktywne środki i ścisłe ramy czasowe, były zrównoważone gwarancjami praw podstawowych, a zwłaszcza wolności słowa. Zainteresowane strony zwróciły uwagę na szereg niezbędnych środków dotyczących przejrzystości, odpowiedzialności oraz konieczności nadzoru przez człowieka przy wykorzystywaniu zautomatyzowanych narzędzi.

3.2. Ocena skutków

Rada ds. Kontroli Regulacyjnej wydała pozytywną opinię z zastrzeżeniami w sprawie oceny skutków i przedstawiła szereg różnych zaleceń dotyczących usprawnień[5]. Po wydaniu tej opinii sprawozdanie z oceny skutków zostało zmienione, aby uwzględnić główne uwagi Rady ds. Kontroli Regulacyjnej, poprzez położenie szczególnego nacisku na treści o charakterze terrorystycznym, a jednocześnie jeszcze silniejsze podkreślenie skutków dla funkcjonowania jednolitego rynku cyfrowego, jak również przedstawienie bardziej dogłębnej analizy wpływu na prawa podstawowe i funkcjonowanie gwarancji przewidzianych w wariantach.

Jeżeli nie zostaną wprowadzone dodatkowe środki, spodziewana jest kontynuacja dobrowolnych działań w ramach scenariusza odniesienia i pewne ich skutki dla ograniczenia treści o charakterze terrorystycznym w internecie. Jest jednak mało prawdopodobne, aby

[4] Eurobarometr 469, Nielegalne treści w internecie, czerwiec 2018 r.

[5] Link do opinii Rady ds. Kontroli Regulacyjnej w sprawie RegDoc.

dobrowolne środki zostały wprowadzone przez wszystkich dostawców usług hostingowych narażonych na takie treści, a ponadto oczekuje się dalszego rozdrobnienia prawnego, wprowadzającego dodatkowe bariery dla transgranicznego świadczenia usług. Oprócz scenariusza odniesienia rozważano trzy główne warianty strategiczne, a każdy z nich cechował się coraz większym poziomem skuteczności w realizacji celów określonych w ocenie skutków oraz ogólnego celu politycznego, jakim jest ograniczenie treści o charakterze terrorystycznym w internecie.

Zakres tych zobowiązań we wszystkich trzech wariantach skupiał się na wszystkich dostawcach usług hostingowych (zakres podmiotowy) mających miejsce prowadzenia działalności w UE i w państwach trzecich – o ile oferują oni swoje usługi w Unii (zakres geograficzny). Biorąc pod uwagę charakter problemu i potrzebę uniknięcia nadużywania mniejszych platform, w ramach żadnego z tych wariantów nie przewiduje się żadnych wyłączeń dla MŚP. Wszystkie warianty wymagałyby od dostawców usług hostingowych ustanowienia w UE przedstawiciela prawnego – także w przypadku przedsiębiorstw mających miejsce prowadzenia działalności poza UE – w celu zapewnienia wykonalności przepisów UE. We wszystkich wariantach przewidziano, że państwa członkowskie opracują mechanizmy sankcji.

Wszystkie warianty przewidują utworzenie nowego, zharmonizowanego systemu nakazów usunięcia w odniesieniu do treści o charakterze terrorystycznym w internecie; nakazy te byłyby wydawane przez organy krajowe i kierowane do dostawców usług hostingowych; wszystkie warianty przewidują ponadto wymóg usuwania tych treści w ciągu jednej godziny. Nakazy te niekoniecznie wymagałyby oceny ze strony dostawców usług hostingowych oraz podlegałyby zaskarżeniu.

Gwarancje, w szczególności procedury rozpatrywania skarg i skuteczne środki ochrony prawnej, w tym środki odwoławcze oraz inne przepisy mające na celu zapobieganie błędnemu usuwaniu treści, które nie są treściami o charakterze terrorystycznym, przy jednoczesnym zapewnieniu zgodności z prawami podstawowymi, to wspólne cechy tych trzech wariantów. Ponadto wszystkie warianty obejmują obowiązki sprawozdawcze w postaci przejrzystości publicznej i sprawozdawczości na rzecz państw członkowskich i Komisji, jak również na rzecz organów w przypadku podejrzenia popełnienia przestępstw kryminalnych. Ponadto przewidziano obowiązki w zakresie współpracy między organami krajowymi, dostawcami usług hostingowych i, w stosownych przypadkach, Europolem.

Główne różnice między tymi trzema wariantami dotyczą zakresu definicji treści o charakterze terrorystycznym, stopnia harmonizacji zgłoszeń, zakresu proaktywnych środków, obowiązków koordynacji nałożonych na państwa członkowskie, a także wymogów w zakresie zachowywania danych. Wariant 1 ograniczyłby zakres przedmiotowy do treści rozpowszechnianych w celu bezpośredniego podżegania do popełnienia aktu terrorystycznego, w oparciu o wąską definicję, podczas gdy warianty 2 i 3 przyjęłyby bardziej kompleksowe podejście, obejmujące również materiał dotyczący rekrutacji i szkoleń. Co do proaktywnych środków, w ramach wariantu 1 dostawcy usług hostingowych narażeni na treści o charakterze terrorystycznym musieliby przeprowadzić ocenę ryzyka, ale proaktywne środki w reakcji na to ryzyko pozostałyby dobrowolne. Wariant 2 wymagałby od dostawców usług hostingowych przygotowania planu działań, który może obejmować wykorzystanie automatycznych narzędzi do zapobiegania ponownemu zamieszczaniu już usuniętych treści. Wariant 3 obejmuje bardziej kompleksowe proaktywne środki, zgodnie z którymi dostawcy usług narażeni na treści o charakterze terrorystycznym muszą również identyfikować nowe materiały. We wszystkich wariantach wymogi związane z proaktywnymi środkami byłyby proporcjonalne do poziomu narażenia na materiał terrorystyczny oraz do możliwości

gospodarczych dostawcy usług. Jeśli chodzi o zgłoszenia, wariant 1 nie przyczyniłby się do harmonizacji podejścia do zgłoszeń, natomiast wariant 2 miałby taki wpływ w odniesieniu do Europolu, a wariant 3 dodatkowo obejmowałby zgłoszenia państw członkowskich. W ramach wariantów 2 i 3 państwa członkowskie byłyby zobowiązane do przekazywania informacji, koordynowania i współpracy, a w ramach wariantu 3 musiałyby także zapewnić, aby ich właściwe organy miały zdolność wykrywania i treści o charakterze terrorystycznym i powiadamiania o nich. Wreszcie wariant 3 obejmuje również wymóg zachowania danych jako gwarancję w przypadku błędnego usunięcia oraz w celu ułatwienia prowadzenia śledztw.

Oprócz przepisów prawnych przewidziano, że wszystkim wariantom prawnym towarzyszyć będzie szereg środków wspierających, w szczególności w celu ułatwienia współpracy między organami krajowymi a Europolem, jak również współpracy z dostawcami usług hostingowych oraz wsparcia badań, rozwoju i innowacji na rzecz rozwoju i wdrażania rozwiązań technologicznych. Po przyjęciu instrumentu prawnego można również wdrożyć dodatkowe instrumenty informacyjne i wspierające MŚP.

W ocenie skutków stwierdzono, że realizacja celu polityki wymaga wprowadzenia szeregu środków. Szeroka definicja treści o charakterze terrorystycznym obejmująca najbardziej szkodliwe materiały byłaby korzystniejsza niż wąska definicja treści (wariant 1). Proaktywne obowiązki ograniczone do zapobiegania ponownemu umieszczaniu treści o charakterze terrorystycznym (wariant 2) byłyby mniej skuteczne w porównaniu z obowiązkami związanymi z wykrywaniem nowych treści o charakterze terrorystycznym (wariant 3). Przepisy dotyczące zgłoszeń powinny obejmować zgłoszenia zarówno Europolu, jak i państw członkowskich (wariant 3), a nie ograniczać się wyłącznie do zgłoszeń Europolu (wariant 2), ponieważ zgłoszenia państw członkowskich stanowią istotny wkład w ogólny wysiłek na rzecz ograniczenia dostępności treści o charakterze terrorystycznym w internecie. Środki takie musiałyby zostać wdrożone w uzupełnieniu do środków wspólnych dla wszystkich wariantów, w tym solidnych gwarancji na wypadek błędnego usunięcia treści.

3.3. Prawa podstawowe

Propaganda internetowa terrorystów ma na celu zachęcanie osób do przeprowadzania ataków terrorystycznych, w tym poprzez wyposażenie ich w szczegółowe instrukcje na temat tego, jak wywołać maksymalną szkodę. Po takich okrucieństwach publikowane są kolejne materiały propagandowe służące ich gloryfikowaniu oraz zachęcaniu innych do naśladownictwa. Niniejsze rozporządzenie przyczynia się do ochrony bezpieczeństwa publicznego poprzez ograniczenie dostępności treści o charakterze terrorystycznym, które propagują łamanie praw podstawowych i zachęcają do ich łamania.

Wniosek mógłby potencjalnie wpływać na szereg praw podstawowych:

a) prawa dostawcy treści: prawo do wolności wypowiedzi; prawo do ochrony danych osobowych; prawo do poszanowania życia prywatnego i rodzinnego, zasadę niedyskryminacji oraz prawo do skutecznego środka odwoławczego;

b) prawa dostawcy usług: prawo do wolności prowadzenia działalności gospodarczej; prawo do skutecznego środka odwoławczego;

c) prawa wszystkich obywateli: prawo do wolności wypowiedzi i informacji.

Biorąc pod uwagę odpowiedni dorobek prawny, w rozporządzeniu, którego dotyczy wniosek, zawarto odpowiednie i solidne gwarancje w celu zapewnienia ochrony praw tych osób.

Pierwszy element w związku z tym polega na tym, że rozporządzenie ustanawia definicję treści o charakterze terrorystycznym w internecie zgodnie z definicją przestępstw terrorystycznych zawartą w dyrektywie (UE) 2017/541. Definicja ta ma zastosowanie do nakazów usunięcia, zgłoszeń oraz proaktywnych środków. Definicja ta zapewnia usuwanie wyłącznie nielegalnych treści, które odpowiadają ogólnounijnej definicji przestępstw powiązanych. Ponadto rozporządzenie obejmuje ogólne obowiązki w zakresie staranności dla dostawców usług hostingowych, polegające na zachowaniu należytej staranności, proporcjonalności i działaniu niedyskryminującym wobec przechowywanych przez nich treści, w szczególności przy wdrażaniu własnych warunków w celu uniknięcia usuwania treści, które nie są treściami o charakterze terrorystycznym.

W szczególności rozporządzenie zostało opracowane w taki sposób, aby zapewnić proporcjonalność wprowadzanych środków w odniesieniu do praw podstawowych. W odniesieniu do nakazów usunięcia ocena treści (w tym, w razie konieczności, kontrola legalności) przez właściwy organ uzasadnia godzinny termin usunięcia w przypadku tego środka. Ponadto przepisy niniejszego rozporządzenia odnoszące się do zgłoszeń są ograniczone do zgłoszeń przesyłanych przez właściwe organy i organy Unii, w których zawarte są wyjaśnienia, dlaczego treści te można uznać za treści o charakterze terrorystycznym. O ile odpowiedzialność za usuwanie treści wskazanych w zgłoszeniu pozostaje w gestii dostawcy usług hostingowych, decyzję tę ułatwia wspomniana wyżej ocena.

W odniesieniu do proaktywnych środków odpowiedzialność za identyfikację, ocenę i usunięcie treści spoczywa na dostawcach usług hostingowych i są oni zobowiązani do wprowadzenia gwarancji w celu zapewnienia, by treści nie były błędnie usuwane, w tym poprzez nadzór przez człowieka, w szczególności w przypadku konieczności rozpatrzenia szerszego kontekstu. Ponadto, w przeciwieństwie do scenariusza odniesienia, w którym najbardziej dotknięte przedsiębiorstwa tworzą zautomatyzowane narzędzia bez nadzoru przez człowieka, projekt środków i ich wdrożenie podlegałyby obowiązkowi zgłaszania właściwym organom w państwach członkowskich. Obowiązek ten ogranicza ryzyko błędnych usunięć zarówno w przypadku przedsiębiorstw tworzących nowe narzędzia, jak i w przypadku przedsiębiorstw, które już z nich korzystają. Ponadto dostawcy usług hostingowych mają obowiązek zapewnić przyjazne dla użytkownika mechanizmy rozpatrywania skarg dla dostawców treści, aby mogli oni zaskarżyć decyzję o usunięciu ich treści, a także obowiązek publikować sprawozdania na temat przejrzystości dla ogółu społeczeństwa.

Wreszcie, gdyby jakiekolwiek treści i związane z nimi dane zostały błędnie usunięte pomimo tych gwarancji, podmioty świadczące usługi hostingowe są zobowiązane do zachowania ich przez okres sześciu miesięcy, aby móc przywrócić je w celu zapewnienia skuteczności procedury rozpatrywania skarg i procedury odwoławczej, mając na względzie ochronę wolności wypowiedzi i informacji. Jednocześnie zachowywanie treści przyczynia się również do celów egzekwowania prawa. Dostawcy usług hostingowych muszą wprowadzić gwarancje techniczne i organizacyjne w celu zapewnienia, aby dane nie były wykorzystywane do innych celów.

Proponowane środki, w szczególności środki dotyczące nakazów usunięcia, zgłoszeń, proaktywnych środków i zachowywania danych nie tylko powinny chronić użytkowników internetu przed treściami o charakterze terrorystycznym, ale także przyczyniać się do ochrony prawa obywateli do życia poprzez ograniczenie dostępności treści o charakterze terrorystycznym w internecie.

4. WPŁYW NA BUDŻET

Wniosek ustawodawczy dotyczący rozporządzenia nie ma wpływu na budżet Unii.

5. ELEMENTY FAKULTATYWNE

5.1. Plany wdrożenia i monitorowanie, ocena i sprawozdania

W ciągu [jednego roku od daty rozpoczęcia stosowania niniejszego rozporządzenia] Komisja ustanowi szczegółowy program monitorowania produktów, rezultatów i skutków niniejszego rozporządzenia. Program monitorowania określa wskaźniki i środki służące do gromadzenia danych i innych niezbędnych dowodów, a także przedziały czasowe, w jakich będą one gromadzone. Określa się w nim działania, które mają zostać podjęte przez Komisję i państwa członkowskie przy gromadzeniu i analizowaniu danych i innych dowodów w celu monitorowania postępów i dokonania oceny niniejszego rozporządzenia.

Na podstawie ustalonego programu monitorowania w ciągu dwóch lat od wejścia w życie niniejszego rozporządzenia Komisja przedstawi sprawozdanie z wykonania niniejszego rozporządzenia w oparciu o sprawozdania na temat przejrzystości publikowane przez przedsiębiorstwa, jak również informacje dostarczone przez państwa członkowskie. Komisja przeprowadzi ocenę nie wcześniej niż cztery lata po wejściu w życie rozporządzenia.

Na podstawie ustaleń dokonanych w ramach oceny, w tym ustalenia, czy w dalszym ciągu istnieją pewne luki lub zagrożenia, oraz biorąc pod uwagę rozwój technologiczny, Komisja oceni potrzebę rozszerzenia zakresu rozporządzenia. W razie potrzeby Komisja przedłoży wioski mające na celu dostosowanie niniejszego rozporządzenia.

Komisja będzie wspierać wdrażanie, monitorowanie i ocenę rozporządzenia za pośrednictwem grupy ekspertów Komisji. Grupa ta ułatwi również współpracę między dostawcami usług hostingowych, organami ścigania i Europolem; wesprze wymiany i praktyki w zakresie wykrywania i usuwania treści o charakterze terrorystycznym, zapewni wiedzę specjalistyczną na temat zmian trybu funkcjonowania terrorystów w internecie; a także udzieli porad i wskazówek, w stosownych przypadkach, w celu wprowadzenia w życie tych przepisów.

Wdrożenie rozporządzenia, którego dotyczy wniosek, można by ułatwić poprzez szereg środków wspierających. Obejmują one możliwy rozwój platformy w ramach Europolu w celu wsparcia koordynacji zgłoszeń i nakazów usunięcia. Badania finansowane przez UE dotyczące tego, jak zmienia się tryb funkcjonowania terrorystów, poprawiają zrozumienie i podnoszą świadomość wszystkich zainteresowanych stron. Ponadto w ramach programu „Horyzont 2020” wspierane są badania mające na celu rozwój nowych technologii, w tym automatycznego zapobiegania umieszczaniu treści o charakterze terrorystycznym. Ponadto Komisja będzie w dalszym ciągu analizowała, w jaki sposób – za pomocą instrumentów finansowych UE – wspierać właściwe organy i dostawców usług hostingowych we wdrażaniu niniejszego rozporządzenia.

5.2. Szczegółowe objaśnienia poszczególnych przepisów wniosku

W art. 1 określono przedmiot, wskazując, że rozporządzenie ustanawia zasady mające na celu zapobieganie wykorzystywaniu usług hostingowych do rozpowszechniania w internecie treści o charakterze terrorystycznym, w tym obowiązki w zakresie staranności dla dostawców usług

hostingowych oraz środki, które mają wprowadzić państwa członkowskie. Określono w nim także zakres geograficzny, który obejmuje dostawców usług hostingowych świadczących usługi w Unii, niezależnie od ich miejsca prowadzenia działalności.

W art. 2 zawarto definicje terminów użytych we wniosku. W celach prewencyjnych ustanowiono w nim również definicję treści o charakterze terrorystycznym, opierając się na dyrektywie w sprawie zwalczania terroryzmu, której celem jest wychwytywanie materiałów i informacji, które podżegają, zachęcają lub nakłaniają do popełniania przestępstw terrorystycznych lub do ich wspierania, a także dostarczają instrukcji dotyczących popełniania takich przestępstw lub propagują udział w działaniach grupy terrorystycznej.

W art. 3 określono obowiązki w zakresie staranności, których muszą dopełniać dostawcy usług hostingowych przy podejmowaniu działań zgodnie z niniejszym rozporządzeniem, w szczególności z należytym uwzględnieniem odnośnych praw podstawowych. Zawiera on odpowiednie przepisy, które należy wprowadzić do warunków dostawców usług hostingowych, a następnie zapewnić ich stosowanie.

W art. 4 wymaga się, aby państwa członkowskie upoważniły właściwe organy do wydawania nakazów usunięcia oraz nakłada się na dostawców usług hostingowych wymóg usunięcia treści w ciągu jednej godziny po otrzymaniu nakazu usunięcia. Określono w nim również minimalne wymagane elementy, które powinny zawierać nakazy usunięcia, oraz procedury dla dostawców usług hostingowych umożliwiające przekazanie informacji zwrotnych organowi wydającemu, a także informowanie go, jeżeli nie jest możliwe zastosowanie się do nakazu lub jeżeli wymagane są dalsze wyjaśnienia. Zobowiązuje on również organ wydający do informowania organu nadzorującego proaktywne środki o państwie członkowskim jurysdykcji dostawcy usług hostingowych.

W art. 5 ustanawia się wymóg, aby dostawcy usług hostingowych wprowadzili środki służące szybkiemu dokonaniu oceny treści, o których mowa w zgłoszeniu właściwego organu w państwie członkowskim lub organu Unii, nie nakłada się jednak wymogu usuwania treści, o których mowa, ani nie określa się szczegółowych terminów podjęcia działań. Określono w nim również minimalne wymagane elementy, które powinny zawierać zgłoszenia, oraz procedury dla dostawców usług hostingowych umożliwiające przekazanie informacji zwrotnych organowi wydającemu i zwrócenie się o wyjaśnienie do organu, który zgłosił dane treści.

W art. 6 wymaga się od dostawców usług hostingowych wprowadzania, w stosownych przypadkach, skutecznych i proporcjonalnych proaktywnych środków. Określono w nim procedurę zapewniającą, by niektórzy dostawcy usług hostingowych (tj. ci, którzy otrzymali nakaz usunięcia, który stał się prawomocny) wprowadzili dodatkowe proaktywne środki, w przypadku gdy jest to konieczne w celu ograniczenia ryzyka i zgodnie z narażeniem świadczonych przez nich usług na treści o charakterze terrorystycznym. Dostawca usług hostingowych powinien współpracować z właściwym organem w zakresie wymaganych niezbędnych środków, a jeżeli nie można osiągnąć porozumienia, organ może narzucić temu dostawcy usług środki. Artykuł ten określa również procedurę odwoławczą od decyzji organu.

Art. 7 zobowiązuje dostawców usług hostingowych do zachowania usuniętych treści i związanych z nimi danych przez okres sześciu miesięcy na potrzeby postępowań odwoławczych i do celów dochodzeniowych. Okres ten może zostać przedłużony, aby umożliwić zakończenie procedury odwoławczej. Artykuł ten zobowiązuje również

dostawców usług do wprowadzenia gwarancji w celu zapewnienia, by zachowane treści i związane z nimi dane nie były udostępniane lub przetwarzane do innych celów.

Art. 8 nakłada na dostawców usług hostingowych obowiązek wyjaśniania prowadzonej przez nich polityki eliminowania treści o charakterze terrorystycznym oraz publikowania rocznych sprawozdań na temat przejrzystości dotyczących działań podejmowanych w tym zakresie.

Art. 9 przewiduje szczególne gwarancje dotyczące stosowania i wdrażania proaktywnych środków w przypadku stosowania automatycznych narzędzi w celu zapewnienia, aby decyzje były precyzyjne i uzasadnione.

Art. 10 zobowiązuje dostawców usług hostingowych do wdrożenia mechanizmów rozpatrywania skarg dotyczących usunięć, zgłoszeń i proaktywnych środków oraz do bezzwłocznego rozpatrzenia każdej skargi.

W art. 11 ustanawia się obowiązek udostępnienia przez dostawców usług hostingowych dostawcy treści informacji na temat usunięcia, chyba że właściwy organ wymaga, aby nie ujawniać informacji z przyczyn związanych z bezpieczeństwem publicznym.

W art. 12 wymaga się od państw członkowskich zapewnienia, aby właściwe organy dysponowały wystarczającą zdolnością i zasobami na potrzeby wypełniania swoich obowiązków na podstawie niniejszego rozporządzenia.

W art. 13 wymaga się, aby państwa członkowskie współpracowały ze sobą oraz, w stosownych przypadkach, z Europolem, aby uniknąć powielania działań i ingerencji w dochodzenia. Artykuł ten przewiduje również możliwość korzystania przez państwa członkowskie i dostawców usług hostingowych z dedykowanych narzędzi, w tym narzędzi Europolu, w celu przetwarzania nakazów usunięcia i zgłoszeń oraz przekazywania informacji zwrotnych z nimi związanych, a także w celu współpracy w zakresie proaktywnych środków. Nakłada on również na państwa członkowskie wymóg dysponowania odpowiednimi kanałami komunikacji w celu zapewnienia terminowej wymiany informacji przy wdrażaniu i egzekwowaniu przepisów niniejszego rozporządzenia. Artykuł ten zobowiązuje również dostawców usług hostingowych do informowania właściwych organów, gdy dowiedzą się oni o jakichkolwiek dowodach przestępstw terrorystycznych w rozumieniu art. 3 dyrektywy (UE) 2017/541 w sprawie zwalczania terroryzmu.

W art. 14 przewiduje się ustanowienie punktów kontaktowych zarówno przez dostawców usług hostingowych, jak i przez państwa członkowskie w celu ułatwienia komunikacji między nimi, w szczególności w odniesieniu do zgłoszeń i nakazów usunięcia.

W art. 15 ustanowiono jurysdykcję państwa członkowskiego na potrzeby nadzorowania proaktywnych środków, ustalania sankcji i monitorowania.

W art. 16 zobowiązuje się dostawców usług hostingowych, którzy nie mają siedziby w żadnym państwie członkowskim, ale którzy świadczą usługi w Unii, do wyznaczenia przedstawiciela prawnego w Unii.

W art. 17 zobowiązuje się państwa członkowskie do wyznaczenia organów odpowiedzialnych za wydawanie nakazów usunięcia, zgłaszanie treści o charakterze terrorystycznym, nadzorowanie wdrażania proaktywnych środków i egzekwowanie przepisów rozporządzenia.

Art. 18 stanowi, że państwa członkowskie powinny ustanowić przepisy dotyczące sankcji za nieprzestrzeganie przepisów i określono w nim kryteria, które mają uwzględnić państwa członkowskie przy określaniu rodzaju i poziomu sankcji. Biorąc pod uwagę szczególne znaczenie, jakie ma szybkie usuwanie treści o charakterze terrorystycznym zidentyfikowanych w nakazie usunięcia, należy ustanowić szczegółowe przepisy dotyczące sankcji finansowych w przypadku systematycznych naruszeń tego wymogu.

W art. 19 ustanowiono szybszą i bardziej elastyczną procedurę wprowadzania zmian w szablonach nakazów usunięcia i uwierzytelnionych kanałach przekazywania informacji w drodze aktów delegowanych.

W art. 20 określono warunki, na jakich Komisja jest uprawniona do przyjmowania aktów delegowanych w celu zapewnienia koniecznych zmian szablonów i wymogów technicznych dotyczących nakazów usunięcia.

W art. 21 wymaga się od państw członkowskich gromadzenia i przekazywania Komisji określonych informacji dotyczących stosowania rozporządzenia, aby mogła ona wypełniać swoje obowiązki na podstawie art. 23. Komisja ustanowi szczegółowy program monitorowania produktów, rezultatów i skutków rozporządzenia.

Art. 22 stanowi, że Komisja składa sprawozdanie z wykonania niniejszego rozporządzenia dwa lata po jego wejściu w życie.

Art. 23 stanowi, że Komisja składa sprawozdanie z oceny niniejszego rozporządzenia nie wcześniej niż trzy lata po jego wejściu w życie.

Art. 24 stanowi, że rozporządzenie, którego dotyczy wniosek, wejdzie w życie dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym, a następnie zacznie obowiązywać po upływie 6 miesięcy od daty jego wejścia w życie. Termin ten proponuje się z uwagi na konieczność zastosowania środków wykonawczych, a jednocześnie uznając pilną konieczność pełnego stosowania przepisów rozporządzenia, którego dotyczy wniosek. Ten termin wynoszący 6 miesięcy ustalono przy założeniu, że negocjacje zostaną przeprowadzone szybko.

2018/0331 (COD)

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.

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[6],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Niniejsze rozporządzenie ma na celu zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego w otwartym i demokratycznym społeczeństwie poprzez zapobieganie wykorzystywaniu usług hostingowych do celów terrorystycznych. Należy poprawić funkcjonowanie jednolitego rynku cyfrowego poprzez zwiększenie pewności prawa dla dostawców usług hostingowych, podniesienie zaufania użytkowników do środowiska internetowego oraz wzmocnienie gwarancji w odniesieniu do wolności wypowiedzi i informacji.

(2) Dostawcy usług hostingowych działający w internecie odgrywają zasadniczą rolę w gospodarce cyfrowej, łącząc przedsiębiorstwa i obywateli oraz ułatwiając publiczną debatę oraz dystrybucję i otrzymywanie informacji, opinii i pomysłów, co znacząco przyczynia się do innowacji, wzrostu gospodarczego i tworzenia miejsc pracy w Unii. Ich usługi są jednak w niektórych przypadkach wykorzystywane przez osoby trzecie w celu prowadzenia nielegalnej działalności w internecie. Szczególnie niepokojące jest wykorzystywanie dostawców usług hostingowych przez grupy terrorystyczne i ich zwolenników do rozpowszechniania w internecie treści o charakterze terrorystycznym w celu szerzenia swojego przesłania, radykalizacji i rekrutacji oraz ułatwiania działalności terrorystycznej i kierowania nią.

(3) Obecność treści o charakterze terrorystycznym w internecie ma poważne negatywne konsekwencje dla użytkowników, obywateli i ogółu społeczeństwa, jak również dla

[6] Dz.U. C z, s. .

dostawców usług online, u których zamieszczane są tego rodzaju treści, ponieważ podważa zaufanie ich użytkowników i szkodzi ich modelom biznesowym. W świetle ich centralnej roli oraz środków technologicznych i zdolności związanych ze świadczonymi przez nich usługami dostawcy usług internetowych mają szczególne obowiązki społeczne dotyczące ochrony swoich usług przed wykorzystaniem przez terrorystów i pomocy w zwalczaniu treści o charakterze terrorystycznym rozpowszechnianych za pośrednictwem ich usług.

(4) Należy uzupełnić ramy dobrowolnej współpracy między państwami członkowskimi a dostawcami usług hostingowych, poprzez które w 2015 r. zainicjowano wysiłki na poziomie Unii Europejskiej w celu zwalczania treści o charakterze terrorystycznym w internecie, jasnymi ramami prawnymi, aby dalej ograniczyć dostępność treści o charakterze terrorystycznym w internecie i odpowiednio rozwiązać ten szybko narastający problem. Ramy prawne, zgodnie z założeniem, mają opierać się na dobrowolnych wysiłkach, które zostały wzmocnione zaleceniem Komisji (UE) 2018/334[7], i stanowią odpowiedź na wezwania Parlamentu Europejskiego do wzmocnienia środków zwalczania nielegalnych i szkodliwych treści oraz na wezwania Rady Europejskiej do usprawnienia automatycznego wykrywania i usuwania treści, które podżegają do aktów terrorystycznych.

(5) Stosowanie niniejszego rozporządzenia nie powinno mieć wpływu na stosowanie art. 14 dyrektywy 2000/31/WE[8]. W szczególności wszelkie środki wprowadzone przez dostawcę usług hostingowych zgodnie z niniejszym rozporządzeniem, w tym wszelkie proaktywne środki, nie powinny same w sobie prowadzić do utraty przez dostawcę usług zwolnienia od odpowiedzialności przewidzianego w tym przepisie. Niniejsze rozporządzenie nie wpływa na uprawnienia organów i sądów krajowych do ustalenia odpowiedzialności dostawców usług hostingowych w szczególnych przypadkach, gdy nie są spełnione warunki wyłączenia odpowiedzialności na podstawie art. 14 dyrektywy 2000/31/WE.

(6) Zasady mające na celu zapobieganie wykorzystywaniu usług hostingowych do rozpowszechniania w internecie treści o charakterze terrorystycznym, aby zagwarantować sprawne funkcjonowanie rynku wewnętrznego, zostały określone w niniejszym rozporządzeniu przy pełnym poszanowaniu praw podstawowych chronionych w unijnym porządku prawnym, a zwłaszcza praw gwarantowanych w Karcie praw podstawowych Unii Europejskiej.

(7) Niniejsze rozporządzenie przyczynia się do ochrony bezpieczeństwa publicznego, a jednocześnie ustanawia odpowiednie i solidne gwarancje zapewniające ochronę odnośnych praw podstawowych. Obejmuje to prawo do poszanowania życia prywatnego i do ochrony danych osobowych, prawo do skutecznej ochrony sądowej, prawo do wolności wypowiedzi, w tym wolność otrzymywania i przekazywania informacji, prawo do wolności prowadzenia działalności gospodarczej oraz zasadę niedyskryminacji. Właściwe organy i dostawcy usług hostingowych powinni przyjmować wyłącznie środki, które są konieczne, odpowiednie i proporcjonalne w ramach społeczeństwa demokratycznego, biorąc pod uwagę szczególne znaczenie,

[7] Zalecenie Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie (Dz.U. L 63 z 6.3.2018, s. 50).

[8] 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.U. L 178 z 17.7.2000, s. 1).

jakie ma wolność wypowiedzi i informacji, która jest jednym z podstawowych fundamentów pluralistycznego społeczeństwa demokratycznego oraz jedną z wartości, na których opiera się Unia. Środki stanowiące ingerencję w wolność wypowiedzi i informacji powinny być ściśle ukierunkowane w tym sensie, że muszą one służyć zapobieganiu rozpowszechnianiu treści o charakterze terrorystycznym, lecz nie mogą wywierać wpływu na prawo do zgodnego z prawem otrzymywania i udzielania informacji, z uwzględnieniem centralnej roli dostawców usług hostingowych w ułatwianiu debaty publicznej oraz w rozpowszechnianiu i przyjmowaniu faktów, opinii i pomysłów zgodnie z prawem.

(8) Prawo do skutecznego środka odwoławczego zapisano w art. 19 TUE i art. 47 Karty praw podstawowych Unii Europejskiej. Każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed właściwym sądem krajowym przeciwko wszelkim środkom wprowadzonym na podstawie niniejszego rozporządzenia, które mogą negatywnie wpłynąć na prawa tej osoby. Prawo to obejmuje w szczególności możliwość skutecznego zaskarżenia nakazów usunięcia przez dostawców usług hostingowych i dostawców treści przed sądem państwa członkowskiego, którego organy wydały nakaz usunięcia.

(9) W celu zapewnienia jasności w odniesieniu do działań, które zarówno dostawcy usług hostingowych, jak i właściwe organy powinny podejmować, aby zapobiegać rozpowszechnianiu w internecie treści o charakterze terrorystycznym, w niniejszym rozporządzeniu należy w celach prewencyjnych ustanowić definicję treści o charakterze terrorystycznym w oparciu o definicję przestępstw terrorystycznych na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541[9]. Z uwagi na potrzebę przeciwdziałania najbardziej szkodliwej propagandzie terrorystycznej w internecie definicja powinna obejmować materiały i informacje, które podżegają, zachęcają lub nakłaniają do popełniania przestępstw terrorystycznych lub do ich wspierania, a także dostarczają instrukcji dotyczących popełniania takich przestępstw lub propagują udział w działaniach grupy terrorystycznej. Informacje takie obejmują w szczególności tekst, obrazy, nagrania dźwiękowe i nagrania wideo. Oceniając, czy treści stanowią treści o charakterze terrorystycznym w rozumieniu niniejszego rozporządzenia, właściwe organy oraz dostawcy usług hostingowych powinni uwzględniać takie czynniki, jak charakter i treść oświadczeń, kontekst, w jakim oświadczenia zostały sporządzone, oraz to, w jakim stopniu mogą spowodować szkodliwe skutki, a tym samym wpływ na bezpieczeństwo i ochronę osób. Ważny czynnik w tej ocenie stanowi fakt, że dany materiał został wytworzony przez wymienioną w wykazie UE organizację terrorystyczną lub osobę, można go przypisać takiej organizacji lub osobie lub jest rozpowszechniany w imieniu takiej organizacji lub osoby. Treści rozpowszechniane w celach edukacyjnych, dziennikarskich lub badawczych powinny być odpowiednio chronione. Ponadto wyrażanie radykalnych, polemicznych lub kontrowersyjnych poglądów w ramach debaty publicznej na drażliwe kwestie polityczne nie powinno być uznawane za treści o charakterze terrorystycznym.

(10) Aby objąć te internetowe usługi hostingowe, w ramach których rozpowszechniane są treści o charakterze terrorystycznym, niniejsze rozporządzenie powinno mieć zastosowanie do usług społeczeństwa informacyjnego, w ramach których przechowuje

[9] 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.U. L 88 z 31.3.2017, s. 6).

się informacje dostarczone przez usługobiorcę na jego wniosek i udostępnia przechowywane informacje osobom trzecim, niezależnie od tego, czy działalność ta ma charakter czysto techniczny, automatyczny i bierny. Przykładowo do tego rodzaju dostawców usług społeczeństwa informacyjnego można zaliczyć: platformy mediów społecznościowych, transmisję strumieniową wideo, usługi wymiany materiałów wideo, audio i obrazów, wymianę plików i inne usługi w chmurze w zakresie, w jakim udostępniają one informacje osobom trzecim, i strony internetowe, na których użytkownicy mogą zamieszczać komentarze lub recenzje. Rozporządzenie to powinno mieć również zastosowanie do dostawców usług hostingowych mających miejsce prowadzenia działalności poza Unią, ale świadczących usługi na terytorium Unii, ponieważ znaczna część dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym w ramach swoich usług ma miejsce prowadzenia działalności w państwach trzecich. Powinno to zapewnić spełnianie tych samych wymogów przez wszystkie przedsiębiorstwa działające na jednolitym rynku cyfrowym, niezależnie od ich państwa prowadzenia działalności. Ustalenie, czy dostawca usług oferuje usługi w Unii, wymaga przeprowadzenia oceny, czy dostawca usług umożliwia korzystanie ze swoich usług osobom prawnym lub fizycznym w jednym lub kilku państwach członkowskich. Sama tylko dostępność strony internetowej dostawcy usług lub adresu poczty elektronicznej oraz innych danych kontaktowych w jednym lub kilku państwach członkowskich nie powinna być jednak warunkiem wystarczającym do objęcia zakresem zastosowania niniejszego rozporządzenia.

(11) Dla określenia zakresu niniejszego rozporządzenia powinien mieć znaczenie ścisły związek z Unią. Taki ścisły związek z Unią powinno się stwierdzać, jeżeli dostawca usług ma miejsce prowadzenia działalności w Unii lub, jeśli nie, ścisły związek ustala się, jeżeli znaczna liczba użytkowników ulokowana jest w co najmniej jednym państwie członkowskim lub jeżeli działalność jest ukierunkowania na co najmniej jedno państwo członkowskie. To, czy działalność jest kierowana do jednego lub większej liczby państw członkowskich, można ustalić na podstawie wszelkich istotnych okoliczności, w tym takich czynników, jak stosowanie języka lub posługiwanie się walutą danego państwa członkowskiego lub możliwość składania zamówień na towary lub usługi. Kierowanie działalności do któregoś z państw członkowskich może również wynikać z dostępności aplikacji w danym krajowym sklepie z aplikacjami, z obecności reklam na rynku lokalnym lub z posługiwania się w reklamach językiem stosowanym w tym państwie członkowskim, lub z zarządzania relacjami z klientem polegającego np. na obsłudze klientów w języku powszechnie używanym w tym państwie członkowskim. W przypadku gdy usługodawca kieruje swoją działalność do jednego lub kilku państw członkowskich, jak określono w art. 17 ust. 1 lit. c) rozporządzenia (WE) nr 1215/2012 Parlamentu Europejskiego i Rady[10], należy również założyć ścisły związek. Z drugiej strony, świadczenie usługi w związku ze zwykłym przestrzeganiem zakazu dyskryminacji ustanowionego w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/302[11] nie może być

[10] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz.U. L 351 z 20.12.2012, s. 1).

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/302 z dnia 28 lutego 2018 r. w sprawie nieuzasadnionego blokowania geograficznego oraz innych form dyskryminacji klientów ze względu na przynależność państwową, miejsce rezydowania lub miejsce prowadzenia działalności na rynku

samo w sobie uważane za kierowanie lub ukierunkowywanie działalności na dane terytorium w Unii.

(12) Dostawcy usług hostingowych powinni dopełniać określonych obowiązków w zakresie staranności, aby zapobiec rozpowszechnianiu treści o charakterze terrorystycznym w ramach swoich usług. Te obowiązki w zakresie staranności nie powinny sprowadzać się do ogólnego obowiązku monitorowania. Obowiązki w zakresie staranności obejmują przy stosowaniu przez dostawców usług hostingowych niniejszego rozporządzenia zachowanie przez nich należytej staranności, proporcjonalności i niedyskryminowania w działaniach wobec przechowywanych przez nich treści, w szczególności przy wdrażaniu własnych warunków w celu uniknięcia usuwania treści, które nie są treściami o charakterze terrorystycznym. Usuwanie lub uniemożliwianie dostępu musi odbywać się z poszanowaniem wolności wypowiedzi i informacji.

(13) Procedura i obowiązki wynikające ze skierowanych do dostawców usług hostingowych nakazów usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich po przeprowadzeniu oceny przez właściwe organy powinny zostać zharmonizowane. Państwa członkowskie powinny zachować swobodę wyboru właściwych organów, która umożliwi im wyznaczenie w tym celu organów administracyjnych, organów ścigania lub organów sądowych. Biorąc pod uwagę prędkość, z jaką treści o charakterze terrorystycznym są rozpowszechniane w internecie, przepis ten nakłada na dostawców usług hostingowych obowiązek zapewnienia usunięcia treści o charakterze terrorystycznym zidentyfikowanych w nakazie usunięcia lub uniemożliwienia dostępu do nich w ciągu jednej godziny od otrzymania nakazu usunięcia. To do dostawców usług hostingowych należy decyzja, czy usunąć dane treści, czy też uniemożliwić dostęp do tych treści użytkownikom w Unii.

(14) Właściwy organ powinien przekazać nakaz usunięcia bezpośrednio adresatowi i punktowi kontaktowemu za pomocą dowolnego środka elektronicznego zdolnego do sporządzenia pisemnego rejestru na warunkach, które umożliwiają dostawcy usług ustalenie autentyczności, w tym dokładności daty i czasu wysłania i otrzymania nakazu, np. za pośrednictwem zabezpieczonej poczty elektronicznej i platform lub innych zabezpieczonych kanałów, w tym udostępnionych przez dostawcę usług, zgodnie z przepisami dotyczącymi ochrony danych osobowych. Wymóg ten może w szczególności zostać spełniony poprzez korzystanie z kwalifikowanych usług rejestrowanego doręczenia elektronicznego zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014[12].

(15) Zgłoszenia dokonywane przez właściwe organy lub Europol stanowią skuteczny i szybki sposób informowania dostawców usług hostingowych o konkretnych treściach w ramach świadczonych przez nich usług. Mechanizm powiadamiania dostawców usług hostingowych o informacjach, które mogą być uznawane za treści o charakterze terrorystycznym, w celu dobrowolnego rozważenia przez dostawcę zgodności z jego własnymi warunkami powinien pozostać dostępny jako uzupełnienie nakazów usunięcia. Ważne jest, aby dostawcy usług hostingowych traktowali ocenę

---

wewnętrznym oraz w sprawie zmiany rozporządzeń (WE) nr 2006/2004 oraz (UE) 2017/2394 i dyrektywy 2009/22/WE (Dz.U. L 601 z 2.3.2018, s. 1.).

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).

takich zgłoszeń priorytetowo i przekazywali szybkie informacje zwrotne na temat podjętych działań. Ostateczna decyzja dotycząca tego, czy usunąć dane treści, ponieważ nie są zgodne z warunkami dostawcy usług hostingowych, pozostaje w jego gestii. Wdrażając niniejsze rozporządzenie w odniesieniu do zgłoszeń, mandat Europolu, określony w rozporządzeniu (UE) 2016/794[13], pozostaje niezmieniony.

(16) Ze względu na skalę i tempo niezbędne do skutecznego identyfikowania i usuwania treści o charakterze terrorystycznym istotnym elementem w zwalczaniu treści o charakterze terrorystycznym w internecie są proporcjonalne proaktywne środki, w tym w niektórych przypadkach środki zautomatyzowane. W celu zmniejszenia dostępności treści o charakterze terrorystycznym w ramach świadczonych przez siebie usług dostawcy usług hostingowych powinni ocenić, czy należy wprowadzić proaktywne środki, w zależności od zagrożenia i poziomu narażenia na treści o charakterze terrorystycznym, a także od wpływu na prawa osób trzecich i interesu publicznego danych informacji. W związku z tym dostawcy usług hostingowych powinni określić, jakie odpowiednie, skuteczne i proporcjonalne proaktywne środki powinny zostać wdrożone. Wymóg ten nie powinien oznaczać ogólnego obowiązku monitorowania. W kontekście tej oceny brak nakazów usunięcia i zgłoszeń skierowanych do dostawcy usług hostingowych wskazuje na niski poziom narażenia na treści o charakterze terrorystycznym.

(17) Przy wprowadzaniu proaktywnych środków dostawcy usług hostingowych powinni zapewnić zachowanie prawa użytkowników do wolności wypowiedzi i informacji – w tym prawa do swobodnego otrzymywania i przekazywania informacji. Oprócz wszelkich wymogów określonych w prawie, w tym również w przepisach dotyczących ochrony danych osobowych, dostawcy usług hostingowych powinni działać z należytą starannością i wdrażać gwarancje, w tym w szczególności w stosownych przypadkach nadzór i weryfikacje przez człowieka, aby uniknąć jakichkolwiek niezamierzonych i błędnych decyzji prowadzących do usunięcia treści, które nie są treściami o charakterze terrorystycznym. Ma to szczególne znaczenie, gdy dostawcy usług hostingowych wykorzystują zautomatyzowane sposoby wykrywania treści o charakterze terrorystycznym. Wszelkie decyzje o zastosowaniu zautomatyzowanych środków, niezależnie od tego, czy zostały podjęte przez samego dostawcę usług hostingowych czy na wniosek właściwego organu, powinny być oceniane pod kątem wiarygodności wykorzystanej technologii i wpływu na prawa podstawowe.

(18) W celu zapewnienia, aby dostawcy usług hostingowych narażeni na treści o charakterze terrorystycznym wprowadzali odpowiednie środki, by zapobiegać takiemu wykorzystywaniu świadczonych przez nich usług, właściwe organy powinny zwrócić się do dostawców usług hostingowych, którzy otrzymali nakaz usunięcia, który stał się prawomocny, z wnioskiem o przedstawienie informacji na temat przyjętych proaktywnych środków. Mogłyby one obejmować środki zapobiegające ponownemu zamieszczeniu treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony w wyniku otrzymania przez dostawców nakazu usunięcia lub zgłoszenia, przeprowadzające kontrolę w stosunku do narzędzi publicznych lub prywatnych zawierających znane treści o charakterze terrorystycznym. Mogą one również wykorzystywać wiarygodne narzędzia techniczne

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016, s. 53).

do identyfikacji nowych treści o charakterze terrorystycznym, dostępne na rynku albo opracowane przez dostawcę usług hostingowych. Dostawca usług powinien przedstawić sprawozdanie na temat wprowadzonych szczególnych proaktywnych środków, aby umożliwić właściwemu organowi ocenę, czy środki te są skuteczne i proporcjonalne oraz czy, w razie wykorzystywania środków automatycznych, dostawca usług hostingowych posiada niezbędne umiejętności w zakresie nadzoru i weryfikacji przez człowieka. Oceniając skuteczność i proporcjonalność środków, właściwe organy powinny uwzględnić odpowiednie parametry, w tym liczbę nakazów usunięcia i zgłoszeń skierowanych do dostawcy, jego zdolność ekonomiczną oraz wpływ jego usług na rozpowszechnianie treści o charakterze terrorystycznym (na przykład biorąc pod uwagę liczbę użytkowników w Unii).

(19) Po wystąpieniu z wnioskiem właściwy organ powinien nawiązać z dostawcą usług hostingowych dialog na temat koniecznych proaktywnych środków, które należy wdrożyć. W razie konieczności właściwy organ powinien narzucić przyjęcie odpowiednich, skutecznych i proporcjonalnych proaktywnych środków, jeżeli uzna, że dotychczas przyjęte środki są niewystarczające, by wyeliminować zagrożenie. Decyzja o narzuceniu takich szczególnych proaktywnych środków nie powinna co do zasady prowadzić do nałożenia ogólnego obowiązku monitorowania, określonego w art. 15 ust. 1 dyrektywy 2000/31/WE. Biorąc pod uwagę szczególnie poważne zagrożenia związane z rozpowszechnianiem treści o charakterze terrorystycznym, decyzje przyjęte przez właściwe organy na podstawie niniejszego rozporządzenia mogą stanowić odstępstwo od podejścia ustanowionego w art. 15 ust. 1 dyrektywy 2000/31/WE w odniesieniu do niektórych szczególnych, ukierunkowanych środków, których przyjęcie jest niezbędne z uwagi na nadrzędne względy bezpieczeństwa publicznego. Przed przyjęciem takich decyzji właściwy organ powinien zachować równowagę między celami dotyczącymi interesu publicznego a odnośnymi prawami podstawowymi, w tym w szczególności wolnością wypowiedzi i informacji oraz wolnością prowadzenia działalności gospodarczej, a także przedstawić odpowiednie uzasadnienie.

(20) Zobowiązanie dostawców usług hostingowych do zachowania usuniętych treści i związanych z nimi danych powinno być ustanowione do celów szczególnych i ograniczone w czasie do tego, co jest konieczne. Istnieje potrzeba rozszerzenia wymogu zachowania na powiązane dane w takim zakresie, w jakim jakiekolwiek tego rodzaju dane zostałyby utracone w wyniku usunięcia przedmiotowych treści. Powiązane dane mogą obejmować dane takie jak „dane abonenta”, w tym w szczególności dane odnoszące się do tożsamości dostawcy treści oraz „dane dotyczące dostępu”, w tym np. dane o dacie i czasie korzystania przez dostawcę treści lub o logowaniu do serwisu i wylogowaniu się z niego, wraz z adresem IP przydzielonym dostawcy treści przez dostawcę usług dostępu do internetu.

(21) Obowiązek zachowania treści do celów administracyjnego lub sądowego postępowania odwoławczego jest konieczny i uzasadniony w celu zapewnienia skutecznych środków odwoławczych dostawcy treści, którego treści zostały usunięte lub do których dostęp został uniemożliwiony, jak również w celu przywrócenia tych treści w formie sprzed ich usunięcia, w zależności od wyniku procedury odwoławczej. Obowiązek zachowania treści do celów dochodzenia i ścigania jest uzasadniony i konieczny ze względu na wartość, jaką dany materiał mógłby wnieść w celu zakłócenia działalności terrorystycznej lub zapobieżenia jej. W przypadku gdy przedsiębiorstwa usuwają materiał lub uniemożliwiają dostęp do niego, w szczególności za pomocą własnych proaktywnych środków, i nie informują o tym

właściwego organu, ponieważ oceniają, że nie wchodzi to w zakres art. 13 ust. 4 niniejszego rozporządzenia, organy ścigania mogą nie być świadome istnienia danych treści. Dlatego zachowanie treści do celów zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia dochodzeń i ich ścigania jest również uzasadnione. Do tych celów wymagane zachowanie danych ogranicza się do danych, które mogą mieć związek z przestępstwami terrorystycznymi, a w związku z tym mogą przyczynić się do ścigania przestępstw terrorystycznych lub do zapobiegania poważnemu zagrożeniu bezpieczeństwa publicznego.

(22) W celu zapewnienia proporcjonalności okres zachowania powinien być ograniczony do sześciu miesięcy, aby dać dostawcom treści wystarczająco dużo czasu na rozpoczęcie procedury odwoławczej oraz umożliwić organom ścigania dostęp do odpowiednich danych na potrzeby dochodzenia i ścigania przestępstw terrorystycznych. Okres ten może jednak zostać na wniosek organu prowadzącego postępowanie odwoławcze przedłużony o niezbędny okres, w przypadku gdy wszczęte postępowanie odwoławcze nie zakończyło się w okresie sześciu miesięcy. Okres ten powinien być wystarczający, aby organy ścigania mogły zachować niezbędne dowody w związku z dochodzeniami, a jednocześnie zapewnić równowagę z odpowiednimi prawami podstawowymi.

(23) Niniejsze rozporządzenie nie ma wpływu na gwarancje procesowe ani środki dochodzeniowe dotyczące dostępu do treści i powiązanych danych zachowanych do celów prowadzenia dochodzeń w sprawie przestępstw terrorystycznych i ich ścigania na podstawie prawa krajowego państw członkowskich oraz na podstawie prawodawstwa Unii.

(24) Przejrzystość polityki dostawców usług hostingowych wobec treści o charakterze terrorystycznym ma zasadnicze znaczenie dla zwiększenia ich odpowiedzialności wobec użytkowników oraz podniesienia zaufania obywateli do jednolitego rynku cyfrowego. Dostawcy usług hostingowych powinni publikować roczne sprawozdania na temat przejrzystości zawierające istotne informacje na temat działań podjętych w związku z wykrywaniem, identyfikacją i usuwaniem treści o charakterze terrorystycznym.

(25) Procedury rozpatrywania skarg stanowią niezbędną gwarancję przeciwko błędnemu usuwaniu treści chronionych w ramach wolności wypowiedzi i informacji. W związku z tym dostawcy usług hostingowych powinni ustanowić przyjazne dla użytkownika mechanizmy rozpatrywania skarg oraz zapewnić, by skargi były rozpatrywane bezzwłocznie i przy pełnej przejrzystości wobec dostawcy treści. Wymóg, aby dostawca usług hostingowych przywrócił treści, w przypadku gdy zostały one błędnie usunięte, nie ma wpływu na możliwość egzekwowania przez dostawców usług hostingowych własnych warunków w innych przypadkach.

(26) Skuteczna ochrona prawna, zgodnie z art. 19 TUE i art. 47 Karty praw podstawowych Unii Europejskiej, wymaga, aby osoby były w stanie ustalić powody, dla których treści zamieszczone przez nie zostały usunięte lub dostęp do nich został uniemożliwiony. W tym celu dostawca usług hostingowych powinien udostępnić dostawcy treści istotne informacje umożliwiające dostawcy treści zaskarżenie decyzji. Nie wymaga to jednak powiadomienia dostawcy treści. W zależności od okoliczności dostawcy usług hostingowych mogą zastąpić treści uznane za treści o charakterze terrorystycznym komunikatem, że zostały usunięte lub dostęp do nich został uniemożliwiony zgodnie z niniejszym rozporządzeniem. Na żądanie należy podać dalsze informacje na temat przyczyn oraz możliwości zaskarżenia decyzji przez

dostawcę treści. W przypadku gdy właściwe organy postanowią, że ze względu na bezpieczeństwo publiczne, w tym w kontekście dochodzenia, bezpośrednie powiadamianie dostawcy treści o usunięciu treści lub uniemożliwieniu dostępu do nich uznaje się za niewłaściwe lub przynoszące efekty odwrotne do zamierzonych, powinny poinformować o tym dostawcę usług hostingowych.

(27) W celu uniknięcia powielania działań i ingerencji w dochodzenia właściwe organy powinny przekazywać informacje, koordynować i współpracować ze sobą oraz, w stosownych przypadkach, z Europolem przy wydawaniu nakazów usunięcia lub wysyłaniu zgłoszeń do dostawców usług hostingowych. Przy wdrażaniu przepisów niniejszego rozporządzenia wsparcie mógłby zapewnić Europol, zgodnie ze swoim obecnym mandatem oraz obowiązującymi ramami prawnymi.

(28) W celu zapewnienia skutecznego i wystarczająco spójnego wdrożenia proaktywnych środków właściwe organy w państwach członkowskich powinny współdziałać ze sobą w odniesieniu do rozmów z dostawcami usług hostingowych na temat określania, wdrażania i oceny konkretnych środków proaktywnych. Taka współpraca jest również konieczna w związku z przyjęciem przepisów dotyczących sankcji, a także wdrażania i egzekwowania sankcji.

(29) Ważne jest, aby właściwy organ w państwie członkowskim odpowiedzialnym za nakładanie sankcji był w pełni informowany o wydawaniu nakazów usunięcia i zgłoszeń oraz o późniejszej wymianie informacji między dostawcą usług hostingowych a odpowiednim właściwym organem. W tym celu państwa członkowskie powinny zapewnić odpowiednie kanały komunikacji i mechanizmy umożliwiające szybką wymianę istotnych informacji.

(30) Aby ułatwić szybką wymianę informacji między właściwymi organami, jak również z dostawcami usług hostingowych, oraz aby uniknąć powielania działań, państwa członkowskie mogą korzystać z narzędzi opracowanych przez Europol, takich jak obecna aplikacja zarządzania zgłoszeniami podejrzanych treści w internecie (IRMa) lub narzędzia, które ją zastąpią.

(31) Ze względu na szczególnie poważne konsekwencje niektórych treści o charakterze terrorystycznym dostawcy usług hostingowych powinni niezwłocznie informować organy zainteresowanego państwa członkowskiego lub właściwe organy tam, gdzie mają miejsce prowadzenia działalności lub przedstawiciela prawnego, o wszelkich dowodach dotyczących przestępstw terrorystycznych, o których się dowiedzieli. W celu zapewnienia proporcjonalności obowiązek ten ogranicza się do przestępstw terrorystycznych zdefiniowanych w art. 3 ust. 1 dyrektywy (UE) 2017/541. Obowiązek informowania nie oznacza obowiązku aktywnego poszukiwania takich dowodów przez dostawców usług hostingowych. Zainteresowane państwo członkowskie jest państwem członkowskim, które ma jurysdykcję w zakresie dochodzenia i ścigania przestępstw terrorystycznych na podstawie dyrektywy (UE) 2017/541 w oparciu o obywatelstwo sprawcy lub potencjalnej ofiary przestępstwa lub o miejsce będące celem aktu terrorystycznego. W przypadku wątpliwości dostawcy usług hostingowych mogą przekazywać informacje Europolowi, który powinien postępować zgodnie ze swoim mandatem, w tym przekazywać informacje odpowiednim organom krajowym.

(32) Właściwe organy w państwach członkowskich powinny mieć możliwość korzystania z takich informacji w celu wdrożenia środków dochodzeniowych dostępnych na podstawie prawa państwa członkowskiego lub prawa Unii, w tym wystawiania europejskiego nakazu wydania dowodów na mocy rozporządzenia w sprawie

w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych[14].

(33) Zarówno dostawcy usług hostingowych, jak i państwa członkowskie powinny ustanowić punkty kontaktowe w celu ułatwienia sprawnego rozpatrywania nakazów usunięcia i zgłoszeń. W odróżnieniu od przedstawiciela prawnego punkt kontaktowy służy celom operacyjnym. Punkt kontaktowy dostawcy usług hostingowych powinien obejmować wszelkie wyspecjalizowane środki umożliwiające elektroniczne wnoszenie nakazów usunięcia i dokonywanie zgłoszeń oraz środki techniczne i personalne umożliwiające ich sprawne przetwarzanie. Punkt kontaktowy dostawcy usług hostingowych nie musi znajdować się w Unii, a dostawca usług hostingowych może wyznaczyć istniejący punkt kontaktowy, pod warunkiem że ten punkt kontaktowy jest w stanie pełnić funkcje przewidziane w niniejszym rozporządzeniu. W celu zapewnienia usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich w ciągu jednej godziny od otrzymania nakazu usunięcia dostawcy usług hostingowych powinni zapewnić, by punkt kontaktowy był dostępny 24 godziny na dobę 7 dni w tygodniu. Informacje na temat punktu kontaktowego powinny zawierać informacje o języku, w którym można zwrócić się do punktu kontaktowego. Aby ułatwić komunikację między dostawcami usług hostingowych a właściwymi organami, dostawców usług hostingowych zachęca się do umożliwienia komunikacji w jednym z języków urzędowych Unii, w którym zredagowane są ich warunki.

(34) W przypadku braku ogólnego wymogu, by dostawcy usług zapewniali fizyczną obecność na terytorium Unii, należy zapewnić jasność co do tego, jurysdykcji którego państwa członkowskiego podlega dostawca usług hostingowych oferujący usługi w Unii. Co do zasady dostawca usług hostingowych podlega jurysdykcji państwa członkowskiego, w którym ma główne miejsce prowadzenia działalności lub w którym wyznaczył przedstawiciela prawnego. Niemniej jednak, w przypadku gdy inne państwo członkowskie wydaje nakaz usunięcia, jego organy powinny mieć możliwość egzekwowania swoich nakazów poprzez zastosowanie środków przymusu o charakterze niekarnym, takich jak kary pieniężne. Jeżeli chodzi o dostawców usług hostingowych, którzy nie mają miejsca prowadzenia działalności w Unii i nie wyznaczyli przedstawiciela prawnego, każde państwo członkowskie powinno mieć jednak możliwość nakładania sankcji, pod warunkiem przestrzegania zasady *ne bis in idem*.

(35) Dostawcy usług hostingowych, którzy nie mają miejsca prowadzenia działalności w Unii, powinni wyznaczyć na piśmie przedstawiciela prawnego w celu zapewnienia wypełniania i egzekwowania obowiązków na podstawie niniejszego rozporządzenia.

(36) Przedstawiciel prawny powinien mieć uprawnienia do działania w imieniu dostawcy usług hostingowych.

(37) Do celów niniejszego rozporządzenia państwa członkowskie powinny wyznaczyć właściwe organy. Wymóg wyznaczenia właściwych organów niekoniecznie wiąże się z koniecznością ustanowienia nowych organów, lecz nowe organy mogą być istniejącymi jednostkami odpowiedzialnymi za funkcje określone w niniejszym rozporządzeniu. Niniejsze rozporządzenie wymaga wyznaczenia organów właściwych

[14] COM(2018) 225 final.

do celów wydawania nakazów usunięcia, dokonywania zgłoszeń oraz nadzorowania proaktywnych środków i nakładania sankcji. To państwa członkowskie decydują o tym, ile organów chcą wyznaczyć do tych zadań.

(38) Sankcje są niezbędne do zapewnienia skutecznego wywiązania się przez dostawców usług hostingowych z obowiązków wynikających z niniejszego rozporządzenia. Państwa członkowskie powinny przyjąć przepisy dotyczące sankcji, w tym, w stosownych przypadkach, wytyczne w sprawie nakładania kar pieniężnych. Szczególnie surowe sankcje ustala się w przypadku, gdy dostawca usług hostingowych systematycznie nie usuwa treści o charakterze terrorystycznym lub systematycznie nie uniemożliwia dostępu do nich w ciągu jednej godziny od momentu otrzymania nakazu usunięcia. Nieprzestrzeganie przepisów w poszczególnych przypadkach może być karane przy jednoczesnym przestrzeganiu zasady *ne bis in idem* i zasady proporcjonalności oraz zapewnieniu, by sankcje takie uwzględniały systematyczne nieprawidłowości. Aby zagwarantować pewność prawa, w rozporządzeniu należy określić zakres, w jakim odpowiednie obowiązki mogą podlegać sankcjom. Sankcje za nieprzestrzeganie art. 6 powinny być przyjmowane wyłącznie w odniesieniu do obowiązków wynikających z wniosku o sprawozdanie na podstawie art. 6 ust. 2 lub z decyzji o narzuceniu dodatkowych proaktywnych środków na podstawie art. 6 ust. 4. Przy ustalaniu, czy nałożyć sankcje finansowe, należy odpowiednio uwzględnić zasoby finansowe dostawcy usług. Państwa członkowskie zapewniają, aby sankcje nie zachęcały do usuwania treści, które nie są treściami o charakterze terrorystycznym.

(39) Stosowanie standardowych szablonów ułatwia współpracę i wymianę informacji między właściwymi organami i dostawcami usług, co umożliwia im szybszą i skuteczniejszą komunikację. Szczególnie ważne jest zapewnienie sprawnego działania po otrzymaniu nakazu usunięcia. Szablony obniżają koszty tłumaczenia i przyczyniają się do zapewnienia wysokiego standardu jakości. Formularze odpowiedzi powinny umożliwiać znormalizowaną wymianę informacji, co ma szczególne znaczenie w przypadku, gdy usługodawcy nie są w stanie spełnić wymogów. Uwierzytelnione kanały przekazywania informacji mogą zagwarantować autentyczność nakazu usunięcia, w tym dokładność daty i godziny wysłania i otrzymania nakazu.

(40) W celu umożliwienia, w razie potrzeby, szybkiej zmiany treści szablonów, które mają być stosowane do celów niniejszego rozporządzenia, należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w odniesieniu do zmiany załączników I, II i III do niniejszego rozporządzenia. Aby móc uwzględnić rozwój technologii i powiązanych z nią ram prawnych, Komisja powinna być również uprawniona do przyjmowania aktów delegowanych w celu uzupełnienia niniejszego rozporządzenia o wymogi techniczne dotyczące środków elektronicznych, które mają być stosowane przez właściwe organy do przekazywania nakazów usunięcia. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na szczeblu ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.[15]. W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych,

[15] Dz.U. L 123 z 12.5.2016, s. 1.

instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(41) Państwa członkowskie powinny gromadzić informacje na temat wdrażania prawodawstwa. Na potrzeby oceny prawodawstwa zostanie opracowany szczegółowy program monitorowania produktów, rezultatów i skutków niniejszego rozporządzenia.

(42) W oparciu o ustalenia i wnioski zawarte w sprawozdaniu z wdrażania oraz wyniki monitorowania Komisja powinna przeprowadzić ocenę niniejszego rozporządzenia nie wcześniej niż trzy lata po jego wejściu w życie. Ocena ta powinna opierać się na pięciu kryteriach: skuteczności, efektywności, adekwatności, spójności i europejskiej wartości dodanej. W jej ramach ocenione zostanie funkcjonowanie poszczególnych środków operacyjnych i technicznych przewidzianych w rozporządzeniu, w tym skuteczność środków mających na celu poprawę wykrywania, identyfikacji i usuwania treści o charakterze terrorystycznym, skuteczność mechanizmów ochronnych oraz skutki dla potencjalnie narażonych praw i interesów osób trzecich, włącznie z przeglądem wymogu informowania dostawców treści.

(43) Ponieważ cel niniejszego rozporządzenia, a mianowicie zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego poprzez zapobieganie rozpowszechnianiu w internecie treści o charakterze terrorystycznym, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na rozmiary i skutki ograniczenia możliwe jest jego lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodne z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności, określoną w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

SEKCJA I
PRZEPISY OGÓLNE

Artykuł 1
Przedmiot i zakres stosowania

1. W niniejszym rozporządzeniu ustanawia się jednolite przepisy w celu zapobiegania wykorzystywaniu usług hostingowych do rozpowszechniania w internecie treści o charakterze terrorystycznym. Ustanawia się w nim w szczególności:

   a) przepisy dotyczące obowiązków w zakresie staranności, których mają przestrzegać dostawcy usług hostingowych w celu zapobiegania rozpowszechnianiu treści o charakterze terrorystycznym za pośrednictwem ich usług oraz zapewnienia, w razie potrzeby, szybkiego usuwania tych treści;

   b) zestaw środków, które państwa członkowskie mają wprowadzić w celu identyfikowania treści o charakterze terrorystycznym, umożliwienia ich szybkiego usuwania przez dostawców usług hostingowych i ułatwienia współpracy z właściwymi organami w innych państwach członkowskich, dostawcami usług hostingowych oraz, w stosownych przypadkach, z odpowiednimi organami Unii.

2. Niniejsze rozporządzenie stosuje się do dostawców usług hostingowych świadczących usługi w Unii, niezależnie od ich głównego miejsca prowadzenia działalności.

Artykuł 2
Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „dostawca usług hostingowych” oznacza dostawcę usług społeczeństwa informacyjnego polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek oraz na udostępnianiu przechowywanych informacji osobom trzecim;

2) „dostawca treści” oznacza użytkownika, który dostarczył informacje, które są lub były przechowywane na wniosek użytkownika przez dostawcę usług hostingowych;

3) „oferowanie usług w Unii” oznacza: umożliwianie osobom prawnym lub fizycznym z jednego państwa członkowskiego lub większej ich liczby korzystania z usług dostawcy usług hostingowych, którego z danym państwem członkowskim lub danymi państwami członkowskimi łączy ścisły związek, taki jak:

   a) posiadanie przez dostawcę usług hostingowych miejsca prowadzenia działalności w Unii;

   b) znaczna liczba użytkowników w jednym państwie członkowskim lub większej ich liczbie;

   c) ukierunkowanie prowadzonej działalności na jedno państwo członkowskie lub większą ich liczbę;

4) „przestępstwa terrorystyczne” oznaczają przestępstwa zdefiniowane w art. 3 ust. 1 dyrektywy (UE) 2017/541;

5) „treści o charakterze terrorystycznym” oznaczają informacje należące do co najmniej jednej z następujących kategorii:

   a) podżeganie do popełnienia przestępstw terrorystycznych lub propagowanie popełniania tych przestępstw, w tym poprzez ich gloryfikowanie, a przez to powodowanie ryzyka popełnienia tych czynów;

   b) zachęcanie do przyczyniania się do przestępstw terrorystycznych;

   c) propagowanie działalności grupy terrorystycznej, w szczególności poprzez zachęcenie do udziału w grupie terrorystycznej w rozumieniu art. 2 ust. 3 dyrektywy (UE) 2017/541 lub do jej wspierania;

   d) instruowanie w zakresie metod lub technik do celów popełniania przestępstw terrorystycznych;

6) „rozpowszechnianie treści o charakterze terrorystycznym” oznacza udostępnianie treści o charakterze terrorystycznym osobom trzecim za pośrednictwem usług świadczonych przez dostawców usług hostingowych;

7) „warunki” oznaczają wszystkie warunki i klauzule, niezależnie od ich nazwy lub formy, które regulują stosunek umowny między dostawcą usług hostingowych a ich użytkownikami;

8) „zgłoszenie” oznacza zawiadomienie skierowane przez właściwy organ lub, w stosownych przypadkach, odpowiedni organ Unii do dostawcy usług hostingowych, dotyczące informacji, które można uznać za treści o charakterze terrorystycznym, celem dobrowolnego zbadania przez danego dostawcę zgodności tych informacji z jego własnymi warunkami mającymi na celu zapobieganie rozpowszechnianiu treści o charakterze terrorystycznym;

9) „główne miejsce prowadzenia działalności” oznacza siedzibę główną lub siedzibę statutową, w ramach której wykonywane są główne funkcje finansowe i sprawowany jest nadzór operacyjny.

SEKCJA II
Środki w celu zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym

Artykuł 3
Obowiązki w zakresie staranności

1. Dostawcy usług hostingowych podejmują odpowiednie, rozsądne i proporcjonalne działania zgodnie z niniejszym rozporządzeniem przeciwko rozpowszechnianiu w internecie treści o charakterze terrorystycznym oraz w celu ochrony użytkowników przed treściami o charakterze terrorystycznym. Działają przy tym w sposób staranny, proporcjonalny i niedyskryminacyjny oraz z należytym uwzględnieniem praw podstawowych użytkowników, a także uwzględniają podstawowe znaczenie wolności wypowiedzi i informacji w otwartym i demokratycznym społeczeństwie.

2. Dostawcy usług hostingowych uwzględniają w swoich warunkach i stosują przepisy zapobiegające rozpowszechnianiu treści o charakterze terrorystycznym.

Artykuł 4
Nakazy usunięcia

1. Właściwy organ jest uprawniony do wydania decyzji zobowiązującej dostawcę usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich.

2. Dostawcy usług hostingowych usuwają treści o charakterze terrorystycznym lub uniemożliwiają dostęp do nich w ciągu jednej godziny od momentu otrzymania nakazu usunięcia.

3. Nakazy usunięcia zawierają następujące elementy zgodnie z szablonem określonym w załączniku I:

   a) wskazanie właściwego organu wydającego nakaz usunięcia i potwierdzenie autentyczności nakazu usunięcia przez właściwy organ;

   b) uzasadnienie, dlaczego przedmiotowe treści uznaje się za treści o charakterze terrorystycznym, przynajmniej poprzez odniesienie do kategorii treści o charakterze terrorystycznym wymienionych w art. 2 pkt 5;

   c) ujednolicony format adresowania zasobów (URL) oraz, w razie potrzeby, dodatkowe informacje umożliwiające identyfikację zgłaszanych treści;

d) odesłanie do niniejszego rozporządzenia jako podstawy prawnej nakazu usunięcia;

e) znacznik daty i czasu wystawienia;

f) informacje na temat środków odwoławczych dostępnych dla dostawcy usług hostingowych i dostawcy treści;

g) w stosownych przypadkach – decyzję o nieujawnianiu informacji o usunięciu treści o charakterze terrorystycznym lub uniemożliwieniu dostępu do nich, o której mowa w art. 11.

4. Na wniosek dostawcy usług hostingowych lub dostawcy treści właściwy organ przedstawia szczegółowe uzasadnienie bez uszczerbku dla obowiązku dostawcy usług hostingowych polegającego na wykonaniu nakazu usunięcia w terminie określonym w ust. 2.

5. Właściwe organy kierują nakazy usunięcia do głównego miejsca prowadzenia działalności dostawcy usług hostingowych lub do przedstawiciela prawnego wyznaczonego przez dostawcę usług hostingowych na podstawie art. 16 i przekazują je punktowi kontaktowemu, o którym mowa w art. 14 ust. 1. Nakazy te są wysyłane za pomocą środków elektronicznych zdolnych do sporządzenia pisemnego rejestru na warunkach, które umożliwiają ustalenie autentyczności nadawcy oraz podanie dokładnej daty i czasu wysłania i otrzymania nakazu.

6. Dostawcy usług hostingowych potwierdzają odbiór i bez zbędnej zwłoki informują właściwy organ o usunięciu treści o charakterze terrorystycznym lub uniemożliwieniu dostępu do nich, wskazując w szczególności czas podjęcia działań, z wykorzystaniem szablonu określonego w załączniku II.

7. Jeżeli dostawca usług hostingowych nie jest w stanie wykonać nakazu usunięcia ze względu na siłę wyższą lub faktyczną niemożliwość, których nie można przypisać dostawcy usług hostingowych, informuje o tym bez zbędnej zwłoki właściwy organ, wyjaśniając przyczyny, z wykorzystaniem szablonu określonego w załączniku III. Termin określony w ust. 2 ma zastosowanie od momentu, gdy przywołane przyczyny ustąpią.

8. Jeżeli dostawca usług hostingowych nie jest w stanie wykonać nakazu usunięcia, ponieważ nakaz usunięcia zawiera oczywiste błędy lub nie zawiera informacji wystarczających do wykonania nakazu, informuje o tym bez zbędnej zwłoki właściwy organ, zwracając się o niezbędne wyjaśnienia, z wykorzystaniem szablonu określonego w załączniku III. Termin określony w ust. 2 ma zastosowanie od momentu, gdy wyjaśnienia zostaną przedstawione.

9. Właściwy organ, który wydał nakaz usunięcia, powiadamia właściwy organ, który nadzoruje wdrażanie proaktywnych środków, o których mowa w art. 17 ust. 1 lit. c), kiedy nakaz usunięcia stanie się prawomocny. Nakaz usunięcia staje się prawomocny, jeżeli nie złożono od niego odwołania w terminie zgodnym z mającym zastosowanie prawem krajowym lub jeżeli został on utrzymany w mocy w następstwie odwołania.

Artykuł 5
Zgłoszenia

1. Właściwy organ lub odpowiedni organ Unii mogą skierować zgłoszenie do dostawcy usług hostingowych.

2. Dostawcy usług hostingowych wprowadzają środki operacyjne i techniczne ułatwiające szybką ocenę treści, które zostały zgłoszone przez właściwe organy oraz, w stosownych przypadkach, odpowiednie organy Unii do dobrowolnego rozważenia.

3. Zgłoszenie jest skierowane do głównego miejsca prowadzenia działalności dostawcy usług hostingowych lub do przedstawiciela prawnego wyznaczonego przez dostawcę usług na podstawie art. 16 i przekazywane punktowi kontaktowemu, o którym mowa w art. 14 ust. 1. Zgłoszenia takie są wysyłane za pomocą środków elektronicznych.

4. Zgłoszenie zawiera wystarczająco szczegółowe informacje, w tym powody, dla których treści uważa się za treści o charakterze terrorystycznym, URL oraz, w razie potrzeby, dodatkowe informacje umożliwiające identyfikację zgłaszanych treści o charakterze terrorystycznym.

5. Dostawca usług hostingowych ocenia, w trybie priorytetowym, treści zidentyfikowane w zgłoszeniu w świetle swoich własnych warunków i podejmuje decyzję, czy usunąć te treści lub uniemożliwić dostęp do nich.

6. Dostawca usług hostingowych niezwłocznie informuje właściwy organ lub właściwy organ unijny o wyniku oceny oraz o tym, kiedy podjęto wszelkie działania w wyniku zgłoszenia.

7. W przypadku gdy dostawca usług hostingowych uważa, że zgłoszenie nie zawiera informacji wystarczających do dokonania oceny zgłoszonych treści, niezwłocznie informuje o tym właściwe organy lub właściwy organ Unii, określając, jakie dalsze informacje lub wyjaśnienia są wymagane.

Artykuł 6
Proaktywne środki

1. W stosownych przypadkach dostawcy usług hostingowych wprowadzają proaktywne środki w celu ochrony swoich usług przed rozpowszechnianiem treści o charakterze terrorystycznym. Środki te są skuteczne i proporcjonalne oraz uwzględniają zagrożenie i poziom narażenia na treści o charakterze terrorystycznym, prawa podstawowe użytkowników oraz podstawowe znaczenie wolności wypowiedzi i informacji w otwartym i demokratycznym społeczeństwie.

2. Właściwy organ, o którym mowa w art. 17 ust. 1 lit. c), przypadku gdy został powiadomiony zgodnie z art. 4 ust. 9, zwraca się z wnioskiem do dostawcy usług hostingowych o przedłożenie w terminie trzech miesięcy od otrzymania wniosku, a następnie co najmniej raz w roku, sprawozdania na temat szczególnych proaktywnych środków, które wprowadził, w tym za pomocą zautomatyzowanych narzędzi, w celu:

   a) zapobiegania ponownemu zamieszczaniu treści, które wcześniej zostały usunięte lub do których dostęp został uniemożliwiony, ponieważ uznaje się je za treści o charakterze terrorystycznym;

   b) wykrywania, identyfikacji i szybkiego usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich.

   Wniosek taki wysyła się do głównego miejsca prowadzenia działalności dostawcy usług hostingowych lub do przedstawiciela prawnego wyznaczonego przez dostawcę usług.

Sprawozdania zawierają wszelkie istotne informacje umożliwiające właściwemu organowi, o którym mowa w art. 17 ust. 1 lit. c), ocenę skuteczności i proporcjonalności proaktywnych środków, w tym ocenę funkcjonowania wszelkich wykorzystywanych zautomatyzowanych narzędzi oraz stosowanych mechanizmów weryfikacji i nadzoru przez człowieka.

3. W przypadku gdy właściwy organ, o którym mowa w art. 17 ust. 1 lit. c), uzna, że proaktywne środki wprowadzone i ujęte w sprawozdaniu zgodnie z ust. 2 są niewystarczające do ograniczenia ryzyka i poziomu narażenia oraz do zarządzania tym ryzykiem i poziomem narażenia, może zażądać od dostawcy usług hostingowych wprowadzenia dodatkowych szczególnych proaktywnych środków. W tym celu dostawca usług hostingowych współpracuje z właściwym organem, o którym mowa w art. 17 ust. 1 lit. c), w celu określenia szczególnych środków, jakie dostawca usług hostingowych ma wdrożyć, ustanowienia kluczowych celów i poziomów odniesienia, a także harmonogramu ich wdrożenia.

4. Jeżeli w ciągu trzech miesięcy od zwrócenia się z wnioskiem na podstawie ust. 3 nie można osiągnąć porozumienia, właściwy organ, o którym mowa w art. 17 ust. 1 lit. c), może wydać decyzję o narzuceniu szczególnych dodatkowych niezbędnych i proporcjonalnych proaktywnych środków. W decyzji uwzględnia się w szczególności zdolność ekonomiczną dostawcy usług hostingowych oraz wpływ takich środków na prawa podstawowe użytkowników, a także podstawowe znaczenie wolności wypowiedzi i informacji. Decyzję taką wysyła się do głównego miejsca prowadzenia działalności dostawcy usług hostingowych lub do przedstawiciela prawnego wyznaczonego przez dostawcę usług. Dostawca usług hostingowych regularnie składa sprawozdania z wdrażania takich środków określonych przez właściwy organ, o którym mowa w art. 17 ust. 1 lit. c).

5. Dostawca usług hostingowych może w dowolnym momencie zwrócić się do właściwego organu, o którym mowa w art. 17 ust. 1 lit. c), o przegląd oraz, w stosownych przypadkach, o cofnięcie wniosku lub decyzji odpowiednio na podstawie ust. 2, 3 i 4. Właściwy organ wydaje uzasadnioną decyzję w rozsądnym terminie od otrzymania wniosku od dostawcy usług hostingowych.

Artykuł 7
Zachowanie treści i związanych z nimi danych

1. Dostawcy usług hostingowych zachowują treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony w wyniku nakazu usunięcia, zgłoszenia lub w wyniku proaktywnych środków na podstawie art. 4, 5 i 6, oraz związane z nimi dane, które zostały usunięte w wyniku usunięcia treści o charakterze terrorystycznym, które są konieczne do:

   a) administracyjnego lub sądowego postępowania odwoławczego,

   b) zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania.

2. Treści o charakterze terrorystycznym i związane z nimi dane, o których mowa w ust. 1, zachowuje się przez sześć miesięcy. Treści o charakterze terrorystycznym są, na wniosek właściwego organu lub sądu, zachowywane przez dłuższy okres oraz tak długo, jak jest to konieczne do celów toczącego się postępowania administracyjnego lub sądowego, o którym mowa w ust. 1 lit. a).

3. Dostawcy usług hostingowych zapewniają, aby treści o charakterze terrorystycznym i związane z nimi dane zachowane na podstawie ust. 1 i 2 podlegały odpowiednim gwarancjom technicznym i organizacyjnym.

Wspomniane gwarancje techniczne i organizacyjne zapewniają, by dostęp do zachowanych treści o charakterze terrorystycznym i związanych z nimi danych oraz ich przetwarzanie odbywały się wyłącznie do celów, o których mowa w ust. 1, i zapewniają wysoki poziom ochrony odnośnych danych osobowych. W razie potrzeby dostawcy usług hostingowych dokonują przeglądu i aktualizacji tych gwarancji.

SEKCJA III
GWARANCJE I ODPOWIEDZIALNOŚĆ

Artykuł 8
Obowiązki w zakresie przejrzystości

1. Dostawcy usług hostingowych określają w swoich warunkach własną politykę zapobiegania rozpowszechnianiu treści o charakterze terrorystycznym, w tym, w stosownych przypadkach, rzeczowe wyjaśnienie funkcjonowania proaktywnych środków, w tym wykorzystania zautomatyzowanych narzędzi.
2. Dostawcy usług hostingowych publikują roczne sprawozdania na temat przejrzystości w odniesieniu do podejmowanych działań wymierzonych przeciwko rozpowszechnianiu treści o charakterze terrorystycznym.
3. Sprawozdania na temat przejrzystości zawierają co najmniej następujące informacje:
   a) informacje na temat środków wprowadzonych przez dostawcę usług hostingowych w związku z wykrywaniem, identyfikacją i usuwaniem treści o charakterze terrorystycznym;
   b) informacje na temat środków wprowadzonych przez dostawcę usług hostingowych w celu zapobiegania ponownemu zamieszczaniu treści, które wcześniej zostały usunięte lub do których dostęp został uniemożliwiony, ponieważ uznaje się je za treści o charakterze terrorystycznym;
   c) liczbę przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do takich treści w wyniku odpowiednio nakazów usunięcia, zgłoszeń lub proaktywnych środków;
   d) przegląd i wyniki procedur rozpatrywania skarg.

Artykuł 9
Gwarancje dotyczące stosowania i wdrażania proaktywnych środków

1. Jeżeli dostawcy usług hostingowych korzystają na podstawie niniejszego rozporządzenia ze zautomatyzowanych mechanizmów w odniesieniu do przechowywanych przez siebie treści, dostarczają oni skutecznych i odpowiednich gwarancji zapewniających, by decyzje podejmowane w sprawie takich treści, zwłaszcza decyzje o usunięciu treści uznanych za treści o charakterze terrorystycznym lub o uniemożliwieniu dostępu do nich, były precyzyjne i uzasadnione.

2. Takie gwarancje obejmują przede wszystkim nadzór i weryfikację przez człowieka w przypadkach, gdy jest to właściwe, oraz zawsze, gdy do ustalenia, czy treści należy uznać za treści o charakterze terrorystycznym, czy też nie, wymagana jest szczegółowa ocena danego kontekstu.

Artykuł 10
Mechanizmy rozpatrywania skarg

1. Dostawcy usług hostingowych ustanawiają skuteczne i dostępne mechanizmy umożliwiające dostawcom treści, których treści zostały usunięte lub dostęp do nich uniemożliwiony w wyniku zgłoszenia na podstawie art. 5 lub proaktywnych środków na podstawie art. 6, złożenie skargi na działanie dostawcy usług hostingowych z żądaniem przywrócenia treści.

2. Dostawcy usług hostingowych niezwłocznie rozpatrują każdą skargę, którą otrzymują, i bez zbędnej zwłoki przywracają treści, w przypadku gdy usunięcie lub uniemożliwienie dostępu było nieuzasadnione. Informują oni składającego skargę o wyniku rozpatrzenia skargi.

Artykuł 11
Informacje dla dostawców treści

1. W przypadku gdy dostawcy usług hostingowych usuną treści o charakterze terrorystycznym lub uniemożliwią dostęp do nich, udostępniają oni dostawcy treści informacje na temat takiego usunięcia lub uniemożliwiania dostępu do treści o charakterze terrorystycznym.

2. Na wniosek dostawcy treści dostawca usług hostingowych informuje dostawcę treści o przyczynach usunięcia lub uniemożliwienia dostępu oraz o możliwościach zaskarżenia tej decyzji.

3. Obowiązek na podstawie ust. 1 i 2 nie ma zastosowania, jeżeli właściwy organ zdecyduje, że nie powinno się ujawniać informacji ze względów bezpieczeństwa publicznego, takich jak zapobieganie przestępstwom terrorystycznym, prowadzenie dochodzeń w ich sprawie, wykrywanie i ściganie takich przestępstw, tak długo, jak to konieczne, ale nie dłużej niż [cztery] tygodnie od tej decyzji. W takim przypadku dostawca usług hostingowych nie ujawnia żadnych informacji dotyczących usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich.

SEKCJA IV
Współpraca między właściwymi organami, organami Unii i dostawcami usług hostingowych

Artykuł 12
Zdolności właściwych organów

Państwa członkowskie zapewniają, aby ich właściwe organy dysponowały niezbędnymi zdolnościami i wystarczającymi zasobami, aby osiągnąć cele i wypełnić swoje obowiązki na podstawie niniejszego rozporządzenia.

Artykuł 13

Współpraca między dostawcami usług hostingowych, właściwymi organami oraz, w stosownych przypadkach, odpowiednimi organami Unii

1. Właściwe organy w państwach członkowskich przekazują informacje, koordynują i współpracują ze sobą oraz, w stosownych przypadkach, z odpowiednimi organami Unii takimi jak Europol w odniesieniu do nakazów usunięcia i zgłoszeń w celu uniknięcia powielania działań, a także w celu poprawy koordynacji i uniknięcia ingerencji w dochodzenia prowadzone w różnych państwach członkowskich.

2. Właściwe organy w państwach członkowskich przekazują informacje, koordynują i współpracują z właściwym organem, o którym mowa w art. 17 ust. 1 lit. c) i d), w odniesieniu do środków wprowadzonych na podstawie art. 6 i działań w zakresie egzekwowania prawa na podstawie art. 18. Państwa członkowskie dopilnowują, by właściwy organ, o którym mowa w art. 17 ust. 1 lit. c) i d), posiadał wszystkie istotne informacje. W tym celu państwa członkowskie powinny zapewnić odpowiednie kanały komunikacji lub mechanizmy umożliwiające szybką wymianę istotnych informacji.

3. Państwa członkowskie i dostawcy usług hostingowych mogą zdecydować się na wykorzystanie specjalnych narzędzi, w tym, w stosownych przypadkach, narzędzi ustanowionych przez odpowiednie organy Unii, takie jak Europol, w celu ułatwienia w szczególności:

   a) przetwarzania i informacji zwrotnych dotyczących nakazów usunięcia na podstawie art. 4;

   b) przetwarzania i informacji zwrotnych dotyczących zgłoszeń na podstawie art. 5;

   c) współpracy w celu określenia i wdrożenia proaktywnych środków na podstawie art. 6.

4. W przypadku gdy dostawcy usług hostingowych dowiedzą się o jakichkolwiek dowodach przestępstw terrorystycznych, niezwłocznie informują organy odpowiedzialne za prowadzenie śledztw i ściganie przestępstw w zainteresowanym państwie członkowskim lub punkt kontaktowy w danym państwie członkowskim na podstawie art. 14 ust. 2, w którym mają swoje główne miejsce prowadzenia działalności lub przedstawiciela prawnego. W razie wątpliwości dostawcy usług hostingowych mogą przekazać te informacje Europolowi na potrzeby odpowiednich działań następczych.

Artykuł 14

Punkty kontaktowe

1. Dostawcy usług hostingowych ustanawiają punkt kontaktowy umożliwiający odbiór nakazów usunięcia i zgłoszeń za pomocą środków elektronicznych oraz zapewniają ich szybkie przetwarzanie na podstawie art. 4 i 5. Dopilnowują oni, aby informacje na ten temat były publicznie dostępne.

2. W informacjach, o których mowa w ust. 1, określa się język lub języki urzędowe Unii, o których mowa w rozporządzeniu 1/58, w których można zwracać się do punktu kontaktowego i w których odbywają się dalsze wymiany informacji w związku z nakazami usunięcia i zgłoszeniami na podstawie art. 4 i 5. Obejmują one co najmniej jeden z języków urzędowych państwa członkowskiego, w którym

dostawca usług hostingowych ma swoje główne miejsce prowadzenia działalności lub w którym mieszka lub ma miejsce prowadzenia działalności jego przedstawiciel prawny na mocy art. 16.

3. Państwa członkowskie ustanawiają punkt kontaktowy, który będzie obsługiwać wnioski o wyjaśnienia i informacje zwrotne dotyczące wydanych przez nie nakazów usunięcia i dokonanych zgłoszeń. Informacje na temat punktu kontaktowego są publicznie dostępne.

SEKCJA V
WDROŻENIE I EGZEKWOWANIE

Artykuł 15
Jurysdykcja

1. Państwo członkowskie, w którym znajduje się główne miejsce prowadzenia działalności dostawcy usług hostingowych, ma jurysdykcję do celów art. 6, 18 i 21. Uznaje się, że dostawca usług hostingowych, który nie ma swojego głównego miejsca prowadzenia działalności w jednym z państw członkowskich, podlega jurysdykcji państwa członkowskiego, w którym mieszka lub ma miejsce prowadzenia działalności przedstawiciel prawny, o którym mowa w art. 16.

2. W przypadku gdy dostawca usług hostingowych nie wyznaczy przedstawiciela prawnego, jurysdykcję mają wszystkie państwa członkowskie.

3. W przypadku gdy organ innego państwa członkowskiego wydał nakaz usunięcia zgodnie z art. 4 ust. 1, to państwo członkowskie ma jurysdykcję do zastosowania środków przymusu zgodnie ze swoim prawem krajowym w celu wykonania nakazu usunięcia.

Artykuł 16
Przedstawiciel prawny

1. Dostawca usług hostingowych, który nie ma miejsca prowadzenia działalności w Unii, ale oferuje usługi w Unii, wyznacza na piśmie osobę prawną lub fizyczną jako swojego przedstawiciela prawnego w Unii w celu odbioru, stosowania się do i wykonywania nakazów usunięcia, zgłoszeń, wniosków i decyzji wydanych przez właściwe organy na podstawie niniejszego rozporządzenia. Przedstawiciel prawny rezyduje lub ma siedzibę w jednym z państw członkowskich, w których dostawca usług hostingowych oferuje swoje usługi.

2. Dostawca usług hostingowych powierza przedstawicielowi prawnemu odbiór, stosowanie się do i wykonywanie nakazów usunięcia, zgłoszeń, wniosków i decyzji, o których mowa w ust. 1, w imieniu tego dostawcy usług hostingowych. Dostawcy usług hostingowych przekazują swojemu przedstawicielowi prawnemu uprawnienia i zasoby niezbędne do współpracy z właściwymi organami oraz stosowania się do tych decyzji i nakazów.

3. Wyznaczony przedstawiciel prawny może zostać pociągnięty do odpowiedzialności z tytułu niewywiązania się z obowiązków wynikających z niniejszego rozporządzenia, bez uszczerbku dla odpowiedzialności dostawcy usług hostingowych i postępowań sądowych, które mogą zostać wszczęte przeciwko dostawcy usług hostingowych.

4. Dostawca usług hostingowych powiadamia o wyznaczeniu przedstawiciela prawnego właściwy organ, o którym mowa w art. 17 ust. 1 lit. d), w państwie członkowskim, w którym mieszka lub ma miejsce prowadzenia działalności przedstawiciel prawny. Informacje na temat przedstawiciela prawnego są publicznie dostępne.

SEKCJA VI
PRZEPISY KOŃCOWE

Artykuł 17
Wyznaczenie właściwych organów

1. Każde państwo członkowskie wyznacza właściwy organ lub organy na potrzeby:

   a) wydawania nakazów usunięcia na podstawie art. 4;

   b) wykrywania, identyfikacji i zgłaszania treści o charakterze terrorystycznym dostawcom usług hostingowych na podstawie art. 5;

   c) nadzoru nad wdrażaniem proaktywnych środków na podstawie art. 6;

   d) egzekwowania obowiązków na podstawie niniejszego rozporządzenia poprzez nakładanie sankcji na podstawie art. 18.

2. Najpóźniej do dnia [*sześć miesięcy po wejściu w życie niniejszego rozporządzenia*] państwa członkowskie powiadamiają Komisję o właściwych organach, o których mowa w ust. 1. Komisja publikuje to powiadomienie oraz wszelkie jego zmiany w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 18
Sankcje

1. Państwa członkowskie ustanawiają zasady dotyczące sankcji mających zastosowanie w przypadku niewypełniania obowiązków na podstawie niniejszego rozporządzenia przez dostawców usług hostingowych i wprowadzają wszelkie niezbędne środki w celu zapewnienia ich wdrożenia. Sankcje takie ograniczają się do przypadków niewypełnienia obowiązków wynikających z:

   a) art. 3 ust. 2 (warunki dostawców usług hostingowych);

   b) art. 4 ust. 2 i 6 (wdrożenie i informacja zwrotna na temat nakazów usunięcia);

   c) art. 5 ust. 5 i 6 (ocena i informacja zwrotna na temat zgłoszeń);

   d) art. 6 ust. 2 i 4 (sprawozdania na temat proaktywnych środków oraz przyjęcie środków w następstwie decyzji o narzuceniu szczególnych proaktywnych środków);

   e) art. 7 (zachowywanie danych);

   f) art. 8 (przejrzystość);

   g) art. 9 (gwarancje w odniesieniu do proaktywnych środków);

   h) art. 10 (procedury rozpatrywania skarg);

   i) art. 11 (informacje dla dostawców treści);

   j) art. 13 ust. 4 (informacje na temat dowodów popełnienia przestępstw terrorystycznych);

k) art. 14 ust. 1 (punkty kontaktowe);

l) art. 16 (wyznaczenie przedstawiciela prawnego).

2. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie najpóźniej do dnia ... [*w ciągu sześciu miesięcy od wejścia w życie niniejszego rozporządzenia*] r. powiadamiają Komisję o tych przepisach i środkach, a następnie niezwłocznie powiadamiają ją o wszelkich zmianach mających wpływ na te przepisy.

3. Państwa członkowskie zapewniają, by przy ustalaniu rodzaju i wysokości sankcji właściwe organy uwzględniały wszystkie istotne okoliczności, w tym:

a) charakter, wagę i czas trwania naruszenia;

b) umyślny lub wynikający z zaniedbania charakter naruszenia;

c) wcześniejsze naruszenia popełnione przez pociąganą do odpowiedzialności osobę prawną;

d) kondycja finansowa pociąganej do odpowiedzialności osoby prawnej;

e) poziom współpracy dostawcy usług hostingowych z właściwymi organami.

4. Państwa członkowskie zapewniają, aby systematyczne niedopełnianie obowiązków wynikających z art. 4 ust. 2 podlegało sankcjom finansowym w wysokości do 4 % całkowitych obrotów dostawcy usług hostingowych w ostatnim roku obrotowym.

Artykuł 19
Wymogi techniczne i zmiany szablonów nakazów usunięcia

1. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 20 w celu uzupełnienia niniejszego rozporządzenia o wymogi techniczne dotyczące środków elektronicznych, które mają być stosowane przez właściwe organy do przekazywania nakazów usunięcia.

2. Komisja jest uprawniona do przyjmowania takich aktów delegowanych w celu wprowadzenia zmian w załącznikach I, II i III, by skutecznie zrealizować ewentualną potrzebę poprawienia treści formularzy nakazu usunięcia oraz formularzy wykorzystywanych do przekazywana informacji na temat niemożliwości wykonania nakazu usunięcia.

Artykuł 20
Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 19, powierza się Komisji na czas nieokreślony od dnia [*data stosowania niniejszego rozporządzenia*] r.

3. Przekazanie uprawnień, o którym mowa w art. 19, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w określonym w tej decyzji

późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 19 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie lub gdy przed upływem tego terminu zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 21
Monitorowanie

1. Państwa członkowskie gromadzą od swoich właściwych organów i dostawców usług hostingowych podlegających ich jurysdykcji i co roku przesyłają Komisji do dnia [31 marca] informacje na temat działań, które podjęli zgodnie z niniejszym rozporządzeniem. Informacje te obejmują:

   a) informacje o liczbie wydanych nakazów usunięcia i dokonanych zgłoszeń, o liczbie przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, wraz z odpowiednimi ramami czasowymi na podstawie art. 4 i 5;

   b) informacje dotyczące szczególnych proaktywnych środków wprowadzonych na podstawie art. 6, w tym ilości treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony, oraz odpowiednie ramy czasowe;

   c) informacje dotyczące liczby wszczętych procedur rozpatrywania skarg oraz działań podjętych przez dostawców usług hostingowych na podstawie art. 10;

   d) informacje dotyczące liczby wszczętych procedur odwoławczych oraz decyzji podjętych przez właściwy organ zgodnie z prawem krajowym.

2. Najpóźniej do dnia [*rok po dniu rozpoczęcia stosowania niniejszego rozporządzenia*] r. Komisja ustala szczegółowy program monitorowania produktów, rezultatów i skutków niniejszego rozporządzenia. W programie monitorowania określa się wskaźniki i środki służące do gromadzenia danych i innych niezbędnych dowodów, a także przedziały czasowe, w jakich mają one być gromadzone. Określa się w nim działania, które mają zostać podjęte przez Komisję i państwa członkowskie przy gromadzeniu i analizowaniu danych i innych dowodów w celu monitorowania postępów i dokonania oceny niniejszego rozporządzenia na podstawie art. 23.

Artykuł 22
Sprawozdanie z wdrażania

Do dnia [*dwa lata po wejściu w życie niniejszego rozporządzenia*] r. Komisja składa Parlamentowi Europejskiemu i Radzie sprawozdanie ze stosowania niniejszego

rozporządzenia. Informacje dotyczące monitorowania na podstawie art. 21 oraz informacje wynikające z obowiązków w zakresie przejrzystości na podstawie art. 8 są uwzględniane w sprawozdaniu Komisji. Państwa członkowskie przekazują Komisji informacje niezbędne do przygotowania sprawozdania.

Artykuł 23
Ocena

Nie wcześniej niż w dniu [*trzy lata od daty rozpoczęcia stosowania niniejszego rozporządzenia*] r. Komisja dokonuje oceny niniejszego rozporządzenia i przedstawia Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące stosowania niniejszego rozporządzenia, w tym skuteczności funkcjonowania mechanizmów ochronnych. W stosownych przypadkach sprawozdaniu towarzyszą wnioski ustawodawcze. Państwa członkowskie przekazują Komisji informacje niezbędne do przygotowania sprawozdania.

Artykuł 24
Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Rozporządzenie stosuje się od dnia [6 miesięcy po wejściu w życie] r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*