

Bruksela, 7 grudnia 2018 r.
(OR. en)

15336/18

Międzyinstytucjonalny numer
referencyjny:
2018/0331(COD)

CT 198
ENFOPOL 605
JAI 1264
COTER 175
CYBER 313
TELECOM 461
FREMP 222
AUDIO 121
DROIPEN 199
CODEC 2270

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	6 grudnia 2018 r.
Do:	Delegacje
Nr poprz. dok.:	14978/18 + COR 1
Nr dok. Kom.:	12129/18 + ADD 1-3
Dotyczy:	Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym – podejście ogólne

Na posiedzeniu 6 grudnia 2018 r. Rada uzgodniła podejście ogólne w wersji przedstawionej w załączniku.

Zmiany w stosunku do wniosku Komisji w przypadku fragmentów dodanych zaznaczono ***tlustym drukiem i kursywą***, natomiast tekst usunięty zaznaczono symbolem [...].

[...]

[...] *Projekt*

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym

[...]

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-Społecznego¹,
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.

¹ Dz.U. C z, s. .

- (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, w celu radykalizacji i rekrutacji oraz w celu 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 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 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 mają opierać się na dobrowolnych wysiłkach, które zostały wzmocnione zaleceniem Komisji (UE) 2018/334², 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 podlegają do aktów terrorystycznych.

² 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).

- (5) Stosowanie niniejszego rozporządzenia nie powinno mieć wpływu na stosowanie art. 14 dyrektywy 2000/31/WE³. 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. ***Niniejsze rozporządzenie nie ma zastosowania do działań związanych z bezpieczeństwem narodowym, gdyż kwestia ta pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego.***
- (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.

³ 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).

- (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, jakie ma wolność wypowiedzi i informacji, ***jak również wolność prasy i pluralizm mediów***, które [...] są podstawowymi fundamentami 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 – przez dostawców usług hostingowych i dostawców treści – nakazów usunięcia przed sądem państwa członkowskiego, którego organy wydały nakaz usunięcia ***oraz możliwość zaskarżenia – przez dostawców usług hostingowych – decyzji o narzuceniu proaktywnych środków lub nałożeniu sankcji przed sądem państwa członkowskiego, w którym dostawcy ci mają miejsce prowadzenia działalności lub przedstawiciela prawnego.***

- (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 zawartą w dyrektywie Parlamentu Europejskiego i Rady (UE) 2017/541⁴. Z uwagi na potrzebę przeciwdziałania najbardziej szkodliwej propagandzie terrorystycznej w internecie definicja powinna obejmować materiały [...], które podżegają, zachęcają lub nakłaniają do popełniania przestępstw terrorystycznych lub do ich wspierania [...] lub które propagują udział w działaniach grupy terrorystycznej. [...] **Definicja obejmuje treści, które zawierają wskazówki dotyczące wytwarzania i stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji, jak również substancji CBRJ, lub wskazówki dotyczące innych metod i technik, w tym w zakresie wyboru celów, które to wskazówki mają służyć popełnianiu przestępstw terrorystycznych.** [...] **Materiały** 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, [...] **kontrnarracyjnych** lub badawczych powinny być odpowiednio chronione, **zapewniając odpowiednią równowagę między prawami podstawowymi, w tym w szczególności wolnością wypowiedzi i informacji, a potrzebami w zakresie bezpieczeństwa publicznego. W przypadkach gdy rozpowszechniane materiały publikowane są w ramach odpowiedzialności redakcyjnej dostawcy treści, wszelkie decyzje o usunięciu takich treści powinny uwzględniać standardy dziennikarskie ustanowione na podstawie przepisów dotyczących prasy lub mediów zgodnych z prawem Unii i prawem do wolności wypowiedzi i prawem do wolności i pluralizmu mediów zapisanych w art. 11 Karty praw podstawowych.** Ponadto wyrażanie radykalnych, polemicznych lub kontrowersyjnych poglądów w ramach debaty publicznej na drażliwe kwestie polityczne nie powinno być uznawane za treści o charakterze terrorystycznym.

⁴ 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).

- (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 się informacje *i materiały* dostarczone przez usługobiorcę na jego wniosek i udostępnia przechowywane informacje *i materiały* osobom trzecim, niezależnie od tego, czy działalność ta ma charakter czysto techniczny, automatyczny i bierny. [...] ***Przechowywanie treści polega na przechowywaniu danych w pamięci fizycznego lub wirtualnego serwera; wyłącza to z zakresu stosowania usługi „zwykłego przekazu” i inne usługi łączności elektronicznej w rozumieniu [Europejskiego kodeksu łączności elektronicznej] lub dostawców usług „cachingu”, lub innych dostawców usług na innych poziomach infrastruktury internetowej, takich jak rejestry i podmioty rejestrujące, usługi DNS (system nazw domen) lub usługi pokrewne, takie jak usługi płatnicze lub usługi ochrony przed atakami DDoS (rozproszony atak typu „odmowa usługi”). Ponadto informacje muszą być przechowywane na wniosek dostawcy treści; zakres stosowania obejmuje wyłącznie te usługi, w przypadku których dostawca treści jest bezpośrednim odbiorcą. Wreszcie, przechowywane informacje są udostępniane osobom trzecim, rozumianym jako każdy użytkownik będący osobą trzecią, który nie jest dostawcą treści. Z zakresu stosowania wyłączone są usługi łączności interpersonalnej umożliwiające bezpośrednią i interaktywną wymianę informacji między określoną liczbą osób, w ramach której to wymiany osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach.*** Przykładowo do tego rodzaju dostawców ***usług hostingowych*** [...] można zaliczyć: platformy mediów społecznościowych, usługi transmisji strumieniowej wideo, usługi wymiany materiałów wideo, audio i obrazów, usługi wymiany plików oraz inne usługi przetwarzania w chmurze *i usługi przechowywania* [...]. ***Niniejsze rozporządzenie ma zastosowanie do działalności polegającej na dostarczaniu usług hostingowych, a nie do poszczególnych dostawców lub ich głównej działalności, która może łączyć usługi hostingowe z innymi usługami nieobjętymi zakresem stosowania niniejszego rozporządzenia.***

(10a) 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, jeżeli nie, ścisły związek ustala się, jeżeli znaczna liczba użytkowników ulokowana jest w co najmniej jednym państwie członkowskim lub jeżeli działalność jest ukierunkowana 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 Parlamentu Europejskiego i Rady nr 1215/2012⁵, należy również założyć istnienie ścisłego związku. Z drugiej strony, świadczenie usługi w związku ze zwykłym przestrzeganiem zakazu dyskryminacji ustanowionego w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/302⁶ nie może być samo w sobie uważane za kierowanie lub ukierunkowywanie działalności na dane terytorium w Unii.

⁵ 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).

⁶ 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 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) 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. ***Bez uszczerbku dla wymogu zachowania danych przewidzianego w art. 7 niniejszego rozporządzenia lub w [projekcie aktu prawnego dotyczącego elektronicznego materiału dowodowego], to do dostawców usług hostingowych należy decyzja, czy usunąć dane treści, czy też uniemożliwić dostęp do tych treści użytkownikom w Unii. Powinno to zapobiegać dostępowi lub przynajmniej utrudniać uzyskanie dostępu oraz w zdecydowany sposób zniechęcać użytkowników internetu, którzy korzystają z ich usług, do uzyskiwania dostępu do treści, do których dostęp został uniemożliwiony.***

- (13a) Nakaz usunięcia powinien obejmować klasyfikację danych treści jako treści o charakterze terrorystycznym i zawierać informacje wystarczające do zlokalizowania tych treści, poprzez podanie adresu URL i wszelkich innych dodatkowych informacji, takich jak zrzut ekranu zawierający dane treści. Na wniosek właściwy organ powinien przedstawić dodatkowe uzasadnienie, w którym wyjaśni, dlaczego dane treści uznaje się za treści o charakterze terrorystycznym. W przedstawionym uzasadnieniu można nie zamieszczać informacji szczególnie chronionych, które mogłyby narazić na szwank dochodzenia. Uzasadnienie powinno jednak umożliwiać dostawcy usług hostingowych i, co za tym idzie, dostawcy treści, skuteczne korzystanie z przysługującego im prawa do środka odwoławczego.**
- (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 910/2014⁷.

⁷ 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).

- (15) [...] Mechanizm [...] **zgłoszeniowy**, służący powiadamianiu dostawców usług hostingowych o informacjach **i materiałach**, które mogą być uznawane za treści o charakterze terrorystycznym, w celu dobrowolnego rozważenia przez dostawcę zgodności z jego własnymi warunkami, *stanowi [...] szczególnie skuteczny, szybki i proporcjonalny sposób informowania dostawców usług hostingowych o konkretnych treściach udostępnianych w ramach świadczonych przez nich usług* [...]. Ważne jest, aby dostawcy usług hostingowych traktowali ocenę 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) 2016/794⁸, 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 ryzyka 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 niskie **ryzyko lub** niski poziom narażenia na treści o charakterze terrorystycznym.

⁸ 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).

- (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 weryfikację 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 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 zagrożenia. 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 jakiegokolwiek 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, „*dane transakcyjne*” i [...] „dane dotyczące dostępu”, w tym np. dane o dacie i czasie korzystania przez dostawcę treści lub o logowaniu do usługi i wylogowaniu się z niej, 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, ***narażeni na treści o charakterze terrorystycznym***, powinni publikować roczne sprawozdania na temat przejrzystości zawierające istotne informacje o działaniach podjętych w związku z wykrywaniem, identyfikacją i usuwaniem treści o charakterze terrorystycznym, ***o ile nie jest to sprzeczne z celem wdrożonych środków***.
- (25) Procedury rozpatrywania skarg stanowią niezbędną gwarancję przeciwko błędnemu usuwaniu – ***w wyniku środków zastosowanych zgodnie z warunkami dostawców usług hostingowych*** – 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. ***Ponadto dostawcy treści, których treści zostały usunięte w wyniku nakazu usunięcia, powinni mieć prawo do skutecznego środka odwoławczego zgodnie z art. 19 TUE i art. 47 Karty praw podstawowych Unii Europejskiej***.

- (26) ***W bardziej ogólnym ujęciu, s[...]*** 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 ewentualnego zakłócania dochodzeń właściwe organy powinny przekazywać sobie nawzajem informacje, koordynować działania i współpracować ze sobą oraz, w stosownych przypadkach, z Europolem [...] ***przed*** wydaniem nakazów usunięcia lub ***przy*** wysyłaniu zgłoszeń do dostawców usług hostingowych. [...] ***Podjmując decyzję o wydaniu nakazu usunięcia, właściwy organ powinien należycie uwzględnić wszelkie powiadomienia o konflikcie z interesami dochodzenia („unikanie konfliktu”). Jeśli właściwy organ został poinformowany przez właściwy organ w innym państwie członkowskim o istnieniu nakazu usunięcia, nie powinien wydawać dublującego nakazu.*** 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. ***Komisja powinna ułatwiać taką koordynację i współpracę.***
- (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 [...] ***zachęca się do*** korzystania ze ***specjalnych*** narzędzi opracowanych przez Europol, takich jak obecna aplikacja zarządzania zgłoszeniami podejrzanych treści w internecie (IRMa) lub narzędzia, które ją zastępują.
- (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 europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych⁹.
- (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, **wewnętrzne lub zlecone usługodawcom zewnętrznym**, umożliwiające elektroniczne przekazywanie nakazów usunięcia i dokonywanie zgłoszeń oraz środki techniczne [...] **lub** 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 narażeni na treści o charakterze terrorystycznym, czego dowodzi otrzymanie nakazu usunięcia**, 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. **Mając jednak na uwadze skuteczne wdrażanie, pilny charakter sprawy i porządek publiczny, każde państwo członkowskie powinno mieć jurysdykcję w zakresie nakazów usunięcia i zgłoszeń.**

⁹ COM(2018) 225 final.

- (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. ***Dostawcy usług hostingowych mogą korzystać z dotychczasowego przedstawiciela prawnego, pod warunkiem że ten przedstawiciel prawny jest w stanie pełnić funkcje przewidziane w niniejszym rozporządzeniu.***
- (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 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, **które to sankcje mogą mieć charakter administracyjny lub karny**, 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 ocenie charakteru naruszenia i podejmowaniu decyzji o zastosowaniu sankcji należy w pełni uwzględnić prawa podstawowe, takie jak wolność wypowiedzi.** 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.¹⁰ W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, 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. ***Państwa członkowskie mogą korzystać ze sprawozdań dotyczących przejrzystości przygotowywanych przez dostawców usług hostingowych i w razie konieczności uzupełniać je bardziej szczegółowymi informacjami.*** Na potrzeby oceny prawodawstwa zostanie opracowany szczegółowy program monitorowania produktów, rezultatów i skutków niniejszego rozporządzenia.

¹⁰ Dz.U. L 123 z 12.5. 2016, s. 1.

- (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.
3. ***Niniejsze rozporządzenie nie narusza obowiązku poszanowania praw podstawowych i podstawowych zasad prawnych zapisanych w art. 6 Traktatu o Unii Europejskiej.***

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 posiadanie przez dostawcę usług hostingowych miejsca prowadzenia działalności w Unii;

W razie braku takiego miejsca prowadzenia działalności ocena tego, czy istnieje ścisły związek, opiera się na konkretnych kryteriach faktycznych, takich jak

- a) znaczna liczba użytkowników w jednym państwie członkowskim lub większej ich liczbie;
- b) ***lub*** ukierunkowanie prowadzonej działalności na jedno państwo członkowskie lub większą ich liczbę;
- (4) „przestępstwa terrorystyczne” oznaczają ***jeden z czynów umyślnych wymienionych*** [...] w art. 3 ust. 1 dyrektywy (UE) 2017/541;
- (5) „treści o charakterze terrorystycznym” oznaczają [...] ***material informacyjny, który może przyczynić się do popełnienia czynów umyślnych, wymienionych w art. 3 ust. 1 lit. a)–i) dyrektywy 2017/541, poprzez:***

aa) zagrożenie popełnieniem przestępstwa terrorystycznego;

- a) podżeganie do popełnienia przestępstw terrorystycznych lub propagowanie popełniania tych przestępstw, ***w tym poprzez gloryfikowanie*** [...] ***czynów terrorystycznych***, i tym samym stwarzanie zagrożenia popełnienia takich czynów;
- b) ***zachęcanie osób lub grupy osób do popełnienia lub*** [...] przyczyniania się [...] do przestępstw terrorystycznych;

- c) propagowanie działalności grupy terrorystycznej, w szczególności poprzez ***zachęcenie osób lub grupy osób do*** [...] udziału w ***działalności przestępczej*** [...] grupy terrorystycznej w rozumieniu art. 2 pkt 3 dyrektywy (UE) 2017/541 lub do wspierania tej działalności;

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 **w Unii**.

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 należyтым 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 **zobowiązanie do tego, że nie będą przechowywać treści o charakterze terrorystycznym**, i stosują przepisy zapobiegające rozpowszechnianiu treści o charakterze terrorystycznym.

Artykuł 4

Nakazy usunięcia

1. Właściwy organ jest uprawniony do wydania [...] **nakazu usunięcia** zobowiązującego 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; [...] **ocenę treści** przynajmniej poprzez odniesienie do **odpowiednich** kategorii treści o charakterze terrorystycznym wymienionych w art. 2 pkt 5;

- b) ujednolicony format adresowania zasobów (URL) oraz, w razie potrzeby, dodatkowe informacje umożliwiające identyfikację zgłaszanych treści;
 - c) odesłanie do niniejszego rozporządzenia jako podstawy prawnej nakazu usunięcia;
 - d) znacznik daty i czasu wystawienia;
 - e) informacje na temat środków odwoławczych dostępnych dla dostawcy usług hostingowych i dostawcy treści;
 - f) 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 [...] **dodatkowe** uzasadnienie, **w którym wyjaśnia, dlaczego dane treści uznaje się za treści o charakterze terrorystycznym**, 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. **Bez zbędnej zwłoki, d**[...]ostawcy usług hostingowych potwierdzają odbiór i [...] 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 4a

Procedura konsultacji w przypadku nakazów usunięcia

1. ***Jednocześnie ze zgodnym z art. 4 ust. 5 przekazaniem dostawcom usług hostingowych nakazu usunięcia, organ wydający przekazuje kopię nakazu usunięcia właściwemu organowi, o którym mowa w art. 17 ust. 1 lit. a), państwa członkowskiego, w którym znajduje się główne miejsce prowadzenia działalności dostawcy usług hostingowych***
2. ***W przypadkach gdy właściwy organ państwa członkowskiego, w którym znajduje się główne miejsce prowadzenia działalności dostawcy usług hostingowych, ma uzasadnione podstawy przypuszczać, że przedmiotowy nakaz usunięcia może naruszać podstawowe interesy tego państwa członkowskiego, informuje o tym właściwy organ wydający.***
3. ***Organ wydający bierze te okoliczności pod uwagę i w stosownych przypadkach wycofuje lub dostosowuje nakaz usunięcia.***

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 wystarczające [...] informacje [...] **dotyczące** powodów, dla których treści uznaje się za treści o charakterze terrorystycznym, **oraz podaje** adres URL i, 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 [...] informuje, **bez zbędnej zwłoki**, właściwy organ lub odpowiedni organ Unii 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. [...] Dostawcy usług hostingowych wprowadzają – **w zależności od ryzyka i poziomu narażenia na treści o charakterze terrorystycznym** – proaktywne środki w celu ochrony swoich usług przed rozpowszechnianiem treści o charakterze terrorystycznym. Środki te są skuteczne i proporcjonalne oraz uwzględniają ryzyko 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), w 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) [...] **skutecznego reagowania w przypadku** ponownego **pojawienia się** [...] 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 o charakterze i zakresie proaktywnych środków podejmuje właściwy organ, o którym mowa w art. 17 ust. 1 lit. c), zgodnie z celem niniejszego rozporządzenia.*** 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, usunięte w wyniku usunięcia treści o charakterze terrorystycznym, [...] które to treści i dane 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, [...] **narażeni na treści o charakterze terrorystycznym**, 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 **skutecznego reagowania w przypadku** [...] ponownego **pojawienia się** 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 [...] **sześć tygodni** od tej decyzji. ***W uzasadnionych przypadkach okres ten można przedłużyć jeden raz o kolejnych sześć tygodni.*** 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, [...] **właściwymi** organami Unii*

1. Właściwe organy w państwach członkowskich przekazują informacje, koordynują i współpracują ze sobą oraz, w stosownych przypadkach, z [...] **właściwymi** 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 zakłócania dochodzeń prowadzonych 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. ***Z myślą o skutecznym wdrażaniu niniejszego rozporządzenia oraz uniknięciu powielania działań*** państwa członkowskie i dostawcy usług hostingowych mogą zdecydować się na wykorzystanie specjalnych narzędzi, w tym [...] narzędzi ustanowionych przez [...] ***właściwe*** 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 dochodzeń i ściganie przestępstw w zainteresowanym państwie członkowskim lub zainteresowanych państwach członkowskich [...]. ***Jeżeli nie ma możliwości zidentyfikowania zainteresowanego państwa członkowskiego lub zainteresowanych państw członkowskich***, [...] dostawcy usług hostingowych [...] ***powiadają punkt kontaktowy w danym państwie członkowskim określonym na podstawie art. 14 ust. 3, w którym mają swoje główne miejsce prowadzenia działalności lub przedstawiciela prawnego, a także*** przekazują 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. ***Każde państwo członkowskie ma jurysdykcję do celów art. 4 i 5, niezależnie do tego, gdzie dostawca usług hostingowych ma swoje główne miejsce prowadzenia działalności lub gdzie dostawca usług hostingowych wyznaczył przedstawiciela prawnego.***
2. W przypadku gdy dostawca usług hostingowych nie wyznaczy przedstawiciela prawnego, jurysdykcję mają wszystkie państwa członkowskie. ***Jeżeli państwo członkowskie postanowi wykonywać jurysdykcję, informuje o tym wszystkie pozostałe państwa członkowskie.***

[...] [...]

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 właściwe 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 [*dwanaście* [...] *miesięcy od wejścia w życie niniejszego rozporządzenia*] r. państwa członkowskie powiadamiają Komisję o *właściwym **organie lub*** 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 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 i środki.

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 **fizyczną lub** prawną;

- d) kondycja finansowa pociąganej do odpowiedzialności osoby *fizycznej lub* 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 przekazywania 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 od dnia 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

Sprawozdania z wdrażania

Do dnia ... [*dwa lata od wejścia 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 *[12 [...] miesięcy od wejścia 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
Przewodniczący*

*W imieniu Rady
Przewodniczący*