ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2021/784

z dnia 29 kwietnia 2021 r.

w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym

(Tekst mający znaczenie dla EOG)

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 ([1]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([2]),

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 przeciwdziałanie wykorzystywaniu usług hostingowych do celów terrorystycznych oraz przyczynianie się do poprawy bezpieczeństwa publicznego w całej Unii. Należy poprawić funkcjonowanie jednolitego rynku cyfrowego poprzez zwiększenie pewności prawa dla dostawców usług hostingowych i zwiększenie zaufania użytkowników do środowiska internetowego, a także wzmocnienie gwarancji dotyczących wolności wypowiedzi, w tym wolności otrzymywania i przekazywania informacji i idei w otwartym i demokratycznym społeczeństwie oraz wolności i pluralizmu mediów.

(2) Środki regulacyjne mające przeciwdziałać rozpowszechnianiu w internecie treści o charakterze terrorystycznym powinny zostać uzupełnione strategiami państw członkowskich dotyczącymi walki z terroryzmem, obejmującymi między innymi wzmacnianie umiejętności korzystania z mediów i umiejętności krytycznego myślenia, przedstawianie alternatywnych narracji lub kontrnarracji i inne inicjatywy służące zmniejszeniu wpływu umieszczanych w internecie treści o charakterze terrorystycznym i podatności na te treści, a także inwestycje w pracę społeczną, inicjatywy na rzecz deradykalizacji i kontakty z zainteresowanymi społecznościami, w celu wypracowania trwałego zapobiegania radykalizacji w społeczeństwie.

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

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

([1]) Dz.U. C 110 z 22.3.2019, s. 67.

([2]) Stanowisko Parlamentu Europejskiego z dnia 17 kwietnia 2019 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz stanowisko Rady w pierwszym czytaniu z dnia 16 marca 2021 r. (Dz.U. C 135 z 16.4.2021, s. 1). Stanowisko Parlamentu Europejskiego z dnia 28 kwietnia 2021 r. (dotychczas nieopublikowane w Dzienniku Urzędowym).

(5) Chociaż obecność treści o charakterze terrorystycznym w internecie jest tylko jednym z czynników radykalizacji osób, okazała się ona katalizatorem tej radykalizacji, która może prowadzić do aktów terrorystycznych, a zatem ma poważne negatywne konsekwencje dla użytkowników, obywateli i ogółu społeczeństwa, a także dla dostawców usług hostingowych w internecie, u których zamieszczane są tego rodzaju treści, ponieważ podważa zaufanie ich użytkowników i szkodzi ich modelom biznesowym. Dostawcy usług hostingowych, ze względu na ich kluczową rolę oraz technologiczne środki i zdolności związane ze świadczonymi przez nich usługami, mają szczególne obowiązki wobec społeczeństwa w zakresie ochrony swoich usług przed wykorzystaniem przez terrorystów i udzielania pomocy w przeciwdziałaniu rozpowszechniania w internecie, za pośrednictwem ich usług, treści o charakterze terrorystycznym, z jednoczesnym uwzględnieniem podstawowego znaczenia wolności wypowiedzi, w tym wolności otrzymywania i przekazywania informacji i idei w otwartym i demokratycznym społeczeństwie.

(6) Wysiłki na poziomie Unii w celu zwalczania treści o charakterze terrorystycznym w internecie zainicjowano w 2015 r. poprzez ustanowienie ram dobrowolnej współpracy między państwami członkowskimi a dostawcami usług hostingowych. Wysiłki te należy uzupełnić jasnymi ramami prawnymi, aby w dalszym stopniu ograniczyć dostępność w internecie treści o charakterze terrorystycznym i odpowiednio rozwiązać ten szybko ewoluujący problem. Te ramy prawne mają opierać się na dobrowolnych wysiłkach, które zostały wzmocnione zaleceniem Komisji (UE) 2018/334 ([3]), i stanowią odpowiedź na wezwania Parlamentu Europejskiego do wzmocnienia środków przeciwdziałania nielegalnym i szkodliwym treściom w internecie, zgodnie z ramami horyzontalnymi ustanowionymi w dyrektywie Parlamentu Europejskiego i Rady 2000/31/WE ([4]), a także na wezwania Rady Europejskiej do usprawnienia wykrywania i usuwania treści w internecie, które podżegają do aktów terrorystycznych.

(7) Niniejsze rozporządzenie nie powinno mieć wpływu na stosowanie dyrektywy 2000/31/WE. W szczególności środki podjęte przez dostawcę usług hostingowych zgodnie z niniejszym rozporządzeniem, w tym środki szczególne, nie powinny same w sobie prowadzić do utraty przez tego dostawcę usług hostingowych możliwości skorzystania ze zwolnienia od odpowiedzialności przewidzianego w tej dyrektywie. Ponadto niniejsze rozporządzenie nie ma wpływu na uprawnienia organów i sądów krajowych do ustalenia odpowiedzialności dostawców usług hostingowych w przypadku, gdy nie zostały spełnione warunki zwolnienia od odpowiedzialności określone w tej dyrektywie.

(8) W przypadku konfliktu między niniejszym rozporządzeniem a dyrektywą Parlamentu Europejskiego i Rady 2010/13/UE ([5]) w zakresie przepisów dotyczących audiowizualnych usług medialnych zdefiniowanych w art. 1 pkt 1 lit. a) tej dyrektywy pierwszeństwo powinna mieć dyrektywa 2010/13/UE. Obowiązki wynikające z niniejszego rozporządzenia, w szczególności obowiązki dotyczące dostawców platformy udostępniania wideo, powinny pozostać bez zmian.

(9) W niniejszym rozporządzeniu należy ustanowić przepisy mające na celu przeciwdziałanie wykorzystywaniu usług hostingowych do rozpowszechniania w internecie treści o charakterze terrorystycznym, aby zagwarantować sprawne funkcjonowanie rynku wewnętrznego. Przepisy te powinny zapewniać pełne poszanowanie praw podstawowych chronionych w Unii, a w szczególności praw gwarantowanych w Karcie praw podstawowych Unii Europejskiej (zwanej dalej „Kartą").

(10) Niniejsze rozporządzenie ma przyczyniać się do ochrony bezpieczeństwa publicznego, a jednocześnie mają w nim zostać ustanowione odpowiednie i solidne gwarancje zapewniające ochronę praw podstawowych, w tym prawa do poszanowania życia prywatnego, ochrony danych osobowych, wolności wypowiedzi, w tym wolności otrzymywania i przekazywania informacji, wolności prowadzenia działalności gospodarczej oraz prawa do skutecznego środka prawnego. Ponadto zakazana jest wszelka dyskryminacja. Właściwe organy i dostawcy usług hostingowych powinni przyjmować wyłącznie środki, które są konieczne, odpowiednie i proporcjonalne w społeczeństwie demokratycznym, biorąc pod uwagę szczególne znaczenie, jakie przyznano wolności wypowiedzi i informacji oraz wolności i pluralizmowi mediów, które są podstawowymi fundamentami pluralistycznego społeczeństwa demokratycznego oraz wartościami, na których opiera się Unia. Środki, które mają wpływ na wolność wypowiedzi i informacji, powinny być ściśle ukierunkowane na przeciwdziałanie rozpowszechnianiu w internecie treści o charakterze terrorystycznym, przy poszanowaniu prawa do zgodnego z prawem otrzymywania i przekazywania informacji, z uwzględnieniem centralnej roli dostawców usług hostingowych w ułatwianiu debaty publicznej oraz w rozpowszechnianiu i pozyskiwaniu faktów, opinii i idei zgodnie z prawem. Skuteczne środki internetowe służące przeciwdziałaniu treściom o charakterze terrorystycznym w internecie oraz ochrona wolności wypowiedzi i informacji nie stanowią sprzecznych celów, lecz uzupełniają się i wzajemnie się wzmacniają.

([3]) 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).

([4]) 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).

([5]) Dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) (Dz.U. L 95 z 15.4.2010, s. 1).

(11) W celu zapewnienia jasności w odniesieniu do działań, które zarówno dostawcy usług hostingowych, jak i właściwe organy mają podejmować, aby przeciwdziałać rozpowszechnianiu w internecie treści o charakterze terrorystycznym, należy ustanowić w niniejszym rozporządzeniu, w celach zapobiegawczych, definicję pojęcia „treści o charakterze terrorystycznym", która powinna być spójna z definicjami odpowiednich przestępstw zawartymi w dyrektywie Parlamentu Europejskiego i Rady (UE) 2017/541 ([6]). Z uwagi na potrzebę przeciwdziałania najbardziej szkodliwej propagandzie terrorystycznej w internecie definicja ta powinna obejmować materiały, które podżegają lub nakłaniają kogoś do popełniania przestępstw terrorystycznych lub do przyczynienia się do ich popełniania, materiały, które nakłaniają kogoś do uczestniczenia w działaniach grupy terrorystycznej lub które pochwalają działalność terrorystyczną, w tym poprzez rozpowszechnianie materiałów przedstawiających atak terrorystyczny. Definicja ta powinna także obejmować materiały, które udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji, jak również substancji chemicznych, biologicznych, radiologicznych i jądrowych (CBRJ), lub instruktażu w zakresie innych szczególnych metod lub technik, w tym w zakresie wyboru celów, w celu popełniania przestępstw terrorystycznych lub przyczynienia się do ich popełniania. Materiały takie obejmują tekst, obrazy, nagrania dźwiękowe i nagrania wideo, a także transmisje na żywo przestępstw terrorystycznych, które stwarzają niebezpieczeństwo popełnienia kolejnych takich przestępstw. Oceniając, czy materiały stanowią treści o charakterze terrorystycznym w rozumieniu niniejszego rozporządzenia, właściwe organy oraz dostawcy usług hostingowych powinni uwzględniać takie czynniki, jak charakter i treść komunikatów, kontekst, w jakim komunikaty te zostały przedstawione, oraz to, w jakim stopniu mogą one spowodować szkodliwe skutki dla bezpieczeństwa i ochrony osób. Ważny czynnik w tej ocenie stanowi fakt, że dany materiał został wyprodukowany przez osobę, grupę lub podmiot umieszczone w unijnym wykazie osób, grup i podmiotów uczestniczących w aktach terrorystycznych i podlegających środkom ograniczającym, że można go przypisać takiej osobie, grupie lub podmiotowi lub że jest on rozpowszechniany w imieniu takiej osoby, grupy lub podmiotu.

(12) Materiały rozpowszechniane w celach edukacyjnych, dziennikarskich, artystycznych lub badawczych lub w celu zwiększenia świadomości z myślą o przeciwdziałaniu działalności terrorystycznej nie powinny być uznawane za treści o charakterze terrorystycznym. Ustalając, czy dany materiał dostarczony przez dostawcę treści stanowi „treści o charakterze terrorystycznym" zdefiniowane w niniejszym rozporządzeniu, należy uwzględnić w szczególności prawo do wolność wypowiedzi i informacji, w tym wolność i pluralizm mediów, oraz wolność sztuk i nauk. W szczególności w przypadku gdy dostawca treści ponosi odpowiedzialność redakcyjną, decyzje o usunięciu rozpowszechnionego materiału powinny uwzględniać standardy dziennikarskie ustanowione w przepisach dotyczących prasy lub mediów zgodnie z prawem Unii, w tym Kartą. Ponadto wyrażanie w ramach debaty publicznej radykalnych, polemicznych lub kontrowersyjnych poglądów na drażliwe kwestie polityczne nie powinno być uznawane za treści o charakterze terrorystycznym.

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

(14) Pojęcie „publicznego rozpowszechniania" powinno obejmować udostępnianie informacji potencjalnie nieograniczonej liczbie osób, mianowicie zapewnienie ogółowi użytkowników łatwego dostępu do informacji bez konieczności podejmowania dalszych działań przez dostawcę treści, niezależnie od tego, czy osoby te rzeczywiście korzystają z dostępu do tych informacji. W związku z tym w przypadku gdy dostęp do informacji wymaga rejestracji lub dopuszczenia do udziału w grupie użytkowników, informacje te należy uznawać za publicznie rozpowszechniane jedynie wtedy, gdy użytkownicy poszukujący dostępu do informacji są automatycznie rejestrowani lub dopuszczani do udziału w grupie użytkowników bez konieczności podejmowania decyzji lub dokonywania wyboru przez człowieka co do tego, komu przyznać taki dostęp. Usługi łączności interpersonalnej zdefiniowane w art. 2 pkt 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 ([7]), takie jak usługi poczty elektronicznej lub przesyłania wiadomości prywatnych, nie powinny być objęte zakresem stosowania

([6]) 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).

([7]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz.U. L 321 z 17.12.2018, s. 36).

niniejszego rozporządzenia. Należy uznać, że informacje są przechowywane i publicznie rozpowszechniane w rozumieniu niniejszego rozporządzenia tylko wtedy, gdy takie działania są wykonywane na bezpośredni wniosek dostawcy treści. W związku z tym dostawcy usług takich jak infrastruktura w chmurze – które są świadczone na wniosek stron innych niż dostawcy treści i przynoszą korzyści dostawcom treści jedynie pośrednio – nie powinni być objęci zakresem stosowania niniejszego rozporządzenia. Zakresem stosowania niniejszego rozporządzenia powinni być objęci na przykład dostawcy usług w zakresie mediów społecznościowych, usług wymiany materiałów wideo, obrazów i plików audio, a także usług wymiany plików i innych usług w chmurze, pod warunkiem że usługi te są wykorzystywane do publicznego udostępniania przechowywanych informacji na bezpośredni wniosek dostawcy treści. Jeżeli dostawca usług hostingowych świadczy kilka rodzajów usług, niniejsze rozporządzenie powinno być stosowane wyłącznie do tych usług, które wchodzą w zakres jego stosowania.

(15) Treści o charakterze terrorystycznym są często publicznie rozpowszechniane za pośrednictwem usług świadczonych przez dostawców usług hostingowych mających jednostkę organizacyjną w państwach trzecich. Aby chronić użytkowników w Unii i zapewnić, by wszyscy dostawcy usług hostingowych działający na jednolitym rynku cyfrowym podlegali tym samym wymogom, niniejsze rozporządzenie powinno mieć zastosowanie do wszystkich dostawców odpowiednich usług oferowanych w Unii, niezależnie od państwa, w którym mają oni główną jednostkę organizacyjną. Należy uznać, że dany dostawca usług hostingowych oferuje usługi w Unii, jeżeli umożliwia on osobom fizycznym lub prawnym w co najmniej jednym państwie członkowskim korzystanie z jego usług i którego łączy z tym państwem członkowskim istotny związek.

(16) Uznaje się, że istotny związek z Unią istnieje, jeżeli dostawca usług hostingowych ma jednostkę organizacyjną w Unii, z jego usług korzysta znaczna liczba użytkowników w co najmniej jednym państwie członkowskim lub jeżeli jego działalność jest kierowana do co najmniej jednego państwa członkowskiego. To, czy działalność jest kierowana do co najmniej jednego państwa członkowskiego, należy ustalić na podstawie wszelkich istotnych okoliczności, w tym takich czynników, jak posługiwanie się językiem lub walutą, które są powszechnie używane w danym państwie członkowskim, lub możliwość składania zamówień na towary lub usługi z takiego państwa członkowskiego. Takie kierowanie działalności można również stwierdzić na podstawie dostępności aplikacji w danym krajowym sklepie z aplikacjami, z obecności reklam na rynku lokalnym lub z posługiwania się w reklamach językiem powszechnie używanym w danym państwie członkowskim, lub z zarządzania relacjami z klientem polegającego np. na obsłudze klientów w języku powszechnie używanym w tym państwie członkowskim. W przypadku gdy dostawca usług hostingowych kieruje swoją działalność do co najmniej jednego państwa członkowskiego, jak określono w art. 17 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1215/2012 ([8]), należy również założyć istnienie istotnego związku. Dostępność strony internetowej dostawcy usług hostingowych, adresu poczty elektronicznej lub innych danych kontaktowych w co najmniej jednym państwie członkowskim nie powinna sama w sobie, w oderwaniu od innych czynników, być wystarczająca, aby stanowić istotny związek. Ponadto świadczenie usługi mające na celu jedynie przestrzeganie zakazu dyskryminacji ustanowionego w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/302 ([9]) nie powinno stanowić wyłącznie z tego powodu istotnego związku z Unią.

(17) Należy zharmonizować, po przeprowadzeniu oceny przez właściwe organy, procedurę i obowiązki wynikające z nakazów usunięcia zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia do nich dostępu. Biorąc pod uwagę prędkość, z jaką treści o charakterze terrorystycznym są rozpowszechniane za pośrednictwem usług internetowych, na dostawców usług hostingowych powinien zostać nałożony obowiązek zapewnienia usunięcia treści o charakterze terrorystycznym zidentyfikowanych w nakazie usunięcia lub uniemożliwienia dostępu do takich treści we wszystkich państwach członkowskich w ciągu jednej godziny od otrzymania nakazu usunięcia. Z wyjątkiem należycie uzasadnionych przypadków wyjątkowych właściwy organ powinien udzielić dostawcy usług hostingowych informacji o procedurach i mających zastosowanie terminach z co najmniej 12-godzinnym wyprzedzeniem przed wydaniem wobec tego dostawcy usług hostingowych po raz pierwszy nakazu usunięcia. Należycie uzasadnione przypadki wyjątkowe mają miejsce, gdy usunięcie lub uniemożliwienie dostępu do treści o charakterze terrorystycznym po upływie jednej godziny od otrzymania nakazu usunięcia skutkowałoby poważną szkodą, na przykład w sytuacji bezpośredniego zagrożenia życia lub integralności cielesnej osoby, lub gdy taka treść przedstawia na żywo wydarzenia, których skutkiem jest szkoda stanowiąca zagrożenie życia lub integralności cielesnej osoby. Właściwy organ powinien ustalić, czy przypadki stanowią przypadki wyjątkowe i należycie uzasadnić swoją decyzję w nakazie usunięcia. Jeżeli dostawca usług hostingowych nie jest w stanie wykonać nakazu usunięcia w ciągu godziny od jego otrzymania ze względu na siłę wyższą lub faktyczną niemożliwość, w tym z dających się obiektywnie uzasadnić przyczyn technicznych lub operacyjnych, powinien jak najszybciej poinformować o tym właściwy organ wydający i wykonać nakaz usunięcia, gdy tylko sytuacja zostanie naprawiona

([8]) 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).

([9]) 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 zamieszkania 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 60 I z 2.3.2018, s. 1).

(18) Nakaz usunięcia powinien zawierać uzasadnienie dotyczące uznania materiału, który ma zostać usunięty lub dostęp do którego ma zostać uniemożliwiony, za treści o charakterze terrorystycznym i powinien zawierać informacje wystarczające do zlokalizowania tych treści, poprzez wskazanie dokładnego adresu URL i, w razie potrzeby, wszelkich innych dodatkowych informacji, takich jak zrzut ekranu zawierający dane treści. Uzasadnienie to powinno umożliwiać dostawcy usług hostingowych i, w związku z tym, dostawcy treści, skuteczne skorzystanie z przysługującego im prawa do środka zaskarżenia. W przedstawionym uzasadnieniu nie należy zamieszczać informacji szczególnie chronionych, które mogłyby narazić na szwank trwające postępowania.

(19) Właściwy organ powinien przekazać nakaz usunięcia bezpośrednio punktowi kontaktowemu wyznaczonemu lub ustanowionemu przez dostawcę usług hostingowych do celów niniejszego rozporządzenia za pomocą dowolnego środka elektronicznego dającego możliwość sporządzenia pisemnego potwierdzenia na warunkach, które umożliwiają dostawcy usług hostingowych ustalenie autentyczności nakazu, w tym dokładności daty i godziny jego wysłania i otrzymania, np. za pomocą zabezpieczonej poczty elektronicznej lub platform lub innych zabezpieczonych kanałów, w tym udostępnionych przez dostawcę usług hostingowych, zgodnie z przepisami prawa Unii dotyczącymi ochrony danych osobowych. Spełnienie tego wymogu powinno być możliwe poprzez skorzystanie z, między innymi, kwalifikowanych usług rejestrowanego doręczenia elektronicznego zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([10]). Jeżeli główna jednostka organizacyjna dostawcy usług hostingowych lub miejsce pobytu lub siedziba jego przedstawiciela prawnego znajdują się w państwie członkowskim innym niż państwo członkowskie właściwego organu wydającego, kopię nakazu usunięcia należy przekazać jednocześnie właściwemu organowi tego państwa członkowskiego.

(20) Właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, powinien móc zweryfikować nakaz usunięcia wydany przez właściwe organy innego państwa członkowskiego, by sprawdzić, czy nakaz ten w poważny lub oczywisty sposób nie narusza niniejszego rozporządzenia lub praw podstawowych zapisanych w Karcie. Zarówno dostawca treści, jak i dostawca usług hostingowych powinni mieć prawo wystąpienia z wnioskiem o przeprowadzenie takiej weryfikacji przez właściwy organ w państwie członkowskim, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę. W przypadku wystąpienia z takim wnioskiem, właściwy organ powinien podjąć decyzję stwierdzającą, czy przedmiotowy nakaz usunięcia stanowi takie naruszenie. Jeżeli w decyzji tej stwierdzono takie naruszenie, nakaz usunięcia powinien przestać wywoływać skutki prawne. Przedmiotowa weryfikacja powinna zostać przeprowadzona szybko, aby zapewnić jak najszybsze przywrócenie treści błędnie usuniętych lub do których dostęp został uniemożliwiony.

(21) Dostawcy usług hostingowych narażeni na treści o charakterze terrorystycznym, którzy stosują warunki umowne, powinni umieścić w tych warunkach postanowienia mające przeciwdziałać wykorzystywaniu ich usług do publicznego rozpowszechniania takich treści. Powinni oni stosować te postanowienia z zachowaniem należytej staranności, w sposób przejrzysty, proporcjonalny i niedyskryminacyjny.

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

(23) Przy wdrażaniu środków szczególnych dostawcy usług hostingowych powinni zapewnić zachowanie prawa użytkowników do wolności wypowiedzi i informacji, a także do wolności i pluralizmu mediów podlegających ochronie na mocy Karty. Oprócz wymogów określonych w prawie, w tym w przepisach dotyczących ochrony danych osobowych, dostawcy usług hostingowych powinni działać z należytą starannością i wdrażać zabezpieczenia, w stosownych przypadkach, w tym nadzór i weryfikacje dokonywane przez człowieka, aby uniknąć niezamierzonych lub błędnych decyzji prowadzących do usunięcia lub uniemożliwienia dostępu do treści, które nie są treściami o charakterze terrorystycznym.

([10]) 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).

(24) Dostawca usług hostingowych powinien informować właściwy organ o wdrożonych środkach szczególnych, aby umożliwić temu organowi ustalenie, czy środki te są skuteczne i proporcjonalne oraz czy, w razie wykorzystywania środków automatycznych, dostawca usług hostingowych posiada niezbędne zasoby na potrzeby nadzoru i weryfikacji dokonywanych przez człowieka. Oceniając skuteczność i proporcjonalność środków, właściwe organy powinny uwzględnić odpowiednie parametry, w tym liczbę nakazów usunięcia wydanych wobec dostawcy usług hostingowych, rozmiary i zdolność ekonomiczną dostawcy usług hostingowych oraz wpływ jego usług na rozpowszechnianie treści o charakterze terrorystycznym, na przykład na podstawie liczby użytkowników w Unii, a także zabezpieczenia wprowadzone w celu przeciwdziałania wykorzystywaniu jego usług do rozpowszechniania w internecie treści o charakterze terrorystycznym.

(25) Jeżeli właściwy organ uzna, że wdrożone środki szczególne są niewystarczające, by przeciwdziałać ryzykom, powinien mieć możliwość zażądania przyjęcia dodatkowych odpowiednich, skutecznych i proporcjonalnych środków szczególnych. Żądanie wprowadzenia takich dodatkowych środków szczególnych nie powinno prowadzić do nałożenia ogólnego obowiązku w zakresie nadzoru ani aktywnego poszukiwania faktów w rozumieniu art. 15 ust. 1 dyrektywy 2000/31/WE, ani obowiązku stosowania zautomatyzowanych narzędzi. Jednakże dostawcy usług hostingowych powinni móc stosować zautomatyzowane narzędzia, jeżeli uznają to za stosowne i konieczne do skutecznego przeciwdziałania wykorzystywaniu ich usług do rozpowszechniania w internecie treści o charakterze terrorystycznym.

(26) Obowiązek dostawców usług hostingowych w zakresie zachowywania usuniętych treści i powiązanych z nimi danych powinien być ustanowiony do celów szczególnych i ograniczony do niezbędnego okresu. Istnieje potrzeba rozszerzenia wymogu w zakresie zachowywania na powiązane dane w takim zakresie, w jakim tego rodzaju dane zostałyby utracone w wyniku usunięcia przedmiotowych treści o charakterze terrorystycznym. Powiązane dane mogą obejmować dane takie jak dane abonenta, w szczególności dane odnoszące się do tożsamości dostawcy treści, a także dane dotyczące dostępu, w tym dane o dacie i godzinie skorzystania z usługi przez dostawcę treści i o logowaniu do usługi i wylogowaniu się z niej, wraz z adresem IP przydzielonym dostawcy treści przez dostawcę usług dostępu do internetu.

(27) Obowiązek zachowywania treści do celów kontroli w postępowaniach administracyjnych lub sądowych jest konieczny i uzasadniony ze względu na potrzebę zapewnienia dostawcom treści, których treści zostały usunięte lub do których dostęp został uniemożliwiony, skutecznych środków prawnych, jak również w celu zapewnienia możliwości przywrócenia tych treści w zależności od wyniku tych postępowań. Obowiązek zachowywania materiałów do celów postępowania przygotowawczego lub ścigania jest uzasadniony i konieczny ze względu na wartość, jaką materiały te mogłyby mieć do celów udaremniania działalności terrorystycznej lub zapobiegania jej. Z tego powodu zachowywanie usuniętych treści o charakterze terrorystycznym do celów zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia postepowań przygotowawczych w ich sprawie i ich ścigania powinno być również uznane za uzasadnione. Treści o charakterze terrorystycznym i powiązane z nimi dane powinny być przechowywane jedynie przez okres niezbędny do sprawdzenia przez organy ścigania tych treści o charakterze terrorystycznym i podjęcia decyzji, czy będą one potrzebne do tych celów. Do celów zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania wymagane zachowywanie danych powinno być ograniczone do danych, które mogą mieć związek z przestępstwami terrorystycznymi, i w związku z tym mogłyby przyczynić się do ścigania przestępstw terrorystycznych lub do zapobiegania poważnym zagrożeniom bezpieczeństwa publicznego. W przypadku gdy dostawcy usług hostingowych usuwają materiały lub uniemożliwiają dostęp do nich, w szczególności za pomocą własnych środków szczególnych, powinni oni natychmiast informować właściwe organy o treściach zawierających informacje, które wiążą się z bezpośrednim zagrożeniem życia lub podejrzeniem popełnienia przestępstwa terrorystycznego.

(28) W celu zapewnienia proporcjonalności okres zachowywania powinien być ograniczony do sześciu miesięcy, aby dać dostawcom treści wystarczająco dużo czasu na wszczęcie kontroli w postępowaniach administracyjnych lub sądowych oraz aby umożliwić organom ścigania dostęp do odpowiednich danych na potrzeby prowadzenia postępowań przygotowawczych w sprawie przestępstw terrorystycznych i ich ścigania. Jednakże na wniosek właściwego organu lub sądu, powinno być możliwe przedłużenie tego okresu o niezbędny okres, w przypadku gdy postępowania te nie zakończyły się w okresie sześciu miesięcy. Okres zachowywania powinien być wystarczający, aby organy ścigania mogły zachować niezbędne materiały w związku z postępowaniem przygotowawczym i ściganiem, zapewniając jednocześnie równowagę w zakresie praw podstawowych.

(29) Niniejsze rozporządzenie nie powinno mieć wpływu na gwarancje procesowe ani środki procesowe w postępowaniu przygotowawczym dotyczące dostępu do treści i powiązanych danych zachowanych do celów prowadzenia postępowań przygotowawczych w sprawie przestępstw terrorystycznych i ich ścigania na podstawie prawa Unii lub prawa krajowego.

(30) Przejrzystość zasad dostawców usług hostingowych dotyczących treści o charakterze terrorystycznym ma zasadnicze znaczenie dla zwiększenia ich odpowiedzialności wobec użytkowników oraz podniesienia zaufania obywateli do jednolitego rynku cyfrowego. Dostawcy usług hostingowych, którzy w danym roku kalendarzowym podjęli działania na podstawie niniejszego rozporządzenia lub zostali zobowiązani do podjęcia takich działań, powinni udostępniać publicznie roczne sprawozdania z przejrzystości zawierające informacje o działaniach podjętych w związku z identyfikacją i usuwaniem treści o charakterze terrorystycznym.

(31) Właściwe organy powinny publikować roczne sprawozdania z przejrzystości zawierające informacje o liczbie nakazów usunięcia, liczbie przypadków, w których nakaz nie został wykonany, liczbie decyzji dotyczących środków szczególnych, liczbie przypadków poddanych kontroli w postępowaniu administracyjnym lub sądowym oraz liczbie decyzji w sprawie nałożenia kar.

(32) Prawo do skutecznego środka prawnego jest zapisane w art. 19 Traktatu o Unii Europejskiej (TUE) i w art. 47 Karty. Każda osoba fizyczna lub prawna ma prawo do skutecznego środka prawnego przed właściwym sądem krajowym przeciwko środkom podjętym na podstawie niniejszego rozporządzenia, które mogą negatywnie wpłynąć na prawa tej osoby. Prawo to powinno obejmować w szczególności możliwość skutecznego zaskarżenia przez dostawców usług hostingowych i dostawców treści nakazów usunięcia lub wszelkich decyzji podjętych w wyniku weryfikacji nakazów usunięcia na podstawie niniejszego rozporządzenia przed sądem państwa członkowskiego, którego właściwy organ wydał nakaz usunięcia lub podjął decyzję, oraz możliwość skutecznego zaskarżenia przez dostawców usług hostingowych decyzji dotyczącej środków szczególnych lub kar przed sądem państwa członkowskiego, którego właściwy organ podjął taką decyzję.

(33) Procedury rozpatrywania skarg stanowią niezbędną gwarancję na wypadek błędnego usunięcia treści w internecie lub uniemożliwiania dostępu do nich, w przypadku gdy treści te są chronione 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 bez zbędnej zwłoki i z zachowaniem pełnej przejrzystości wobec dostawcy treści. Nakazanie dostawcy usług hostingowych przywrócenia treści, które zostały błędnie usunięte lub do których dostęp został uniemożliwiony, nie powinno mieć wpływu na możliwość egzekwowania przez dostawcę usług hostingowych własnych warunków umownych.

(34) Skuteczna ochrona prawna zgodnie z art. 19 TUE i art. 47 Karty wymaga, aby dostawcy treści byli w stanie ustalić powody, dla których dostarczone przez nich treści zostały usunięte lub do których dostęp został uniemożliwiony. W tym celu dostawca usług hostingowych powinien udostępnić dostawcy treści informacje dotyczące zaskarżania usunięcia lub uniemożliwienia dostępu. W zależności od okoliczności dostawcy usług hostingowych mogą zastąpić treści, które zostały usunięte lub do których dostęp został uniemożliwiony, komunikatem wskazującym, że treści te zostały usunięte lub dostęp do nich został uniemożliwiony zgodnie z niniejszym rozporządzeniem. Bardziej szczegółowe informacje na temat powodów usunięcia lub uniemożliwienia dostępu oraz środków prawnych wobec usunięcia lub uniemożliwienia dostępu powinny być udzielane na żądanie dostawcy treści. W przypadku gdy właściwe organy postanowią, że ze względu na bezpieczeństwo publiczne, w tym w kontekście prowadzonego postępowania przygotowawczego, bezpośrednie powiadomienie dostawcy treści o usunięciu lub uniemożliwieniu dostępu jest niewłaściwe lub przynosi efekty odwrotne do zamierzonych, powinny poinformować o tym dostawcę usług hostingowych.

(35) Do celów niniejszego rozporządzenia państwa członkowskie powinny wyznaczyć właściwe organy. Powyższe nie oznacza koniecznie ustanowienia nowego organu; powinno być możliwe powierzenie zadań przewidzianych w niniejszym rozporządzeniu istniejącemu organowi. Niniejsze rozporządzenie powinno wymagać wyznaczenia organów właściwych do wydawania nakazów usunięcia, ich weryfikacji oraz nadzorowania środków szczególnych i nakładania kar, podczas gdy państwa członkowskie powinny mieć możliwość decydowania o liczbie właściwych organów, które mają zostać wyznaczone, i o tym, czy mają to być organy administracyjne, organy ścigania czy organy sądowe. Państwa członkowskie powinny zapewnić, by właściwe organy wypełniały swoje zadania w sposób obiektywny i niedyskryminacyjny oraz by nie zwracały się o instrukcje do żadnego innego organu ani nie przyjmowały od niego instrukcji w związku z wykonywaniem zadań powierzonych im na podstawie niniejszego rozporządzenia. Nie powinno to wykluczać sprawowania nadzoru zgodnie z krajowym prawem konstytucyjnym. Państwa członkowskie powinny powiadomić Komisję o właściwych organach wyznaczonych na mocy niniejszego rozporządzenia, a Komisja powinna opublikować w internecie wykaz właściwych organów. Taki wykaz internetowy powinien być łatwo dostępny, tak by dostawcy usług hostingowych mogli szybko weryfikować autentyczność nakazów usunięcia.

(36) W celu uniknięcia powielania wysiłków i ewentualnych konfliktów w zakresie prowadzenia postępowań przygotowawczych, a także w celu ograniczenia do minimum obciążeń spoczywających na dostawcach usług hostingowych, właściwe organy powinny wymieniać się informacjami, koordynować swoje działania i współpracować ze sobą, w stosownych przypadkach włączając w te działania Europol, przed wydaniem nakazów usunięcia. Podejmując decyzję w sprawie wydania nakazu usunięcia, właściwy organ powinien należycie uwzględnić powiadomienia o konflikcie w zakresie prowadzenia postępowań przygotowawczych (unikanie konfliktu). Jeżeli właściwy organ został poinformowany przez właściwy organ innego państwa członkowskiego o istnieniu nakazu usunięcia, nie powinien wydawać nakazu usunięcia w tej samej sprawie. Przy wdrażaniu przepisów niniejszego rozporządzenia wsparcie mógłby zapewnić Europol, zgodnie ze swoim obecnym mandatem i obowiązującymi ramami prawnymi.

(37) W celu zapewnienia skutecznego i wystarczająco spójnego wdrażania środków szczególnych podjętych przez dostawców usług hostingowych właściwe organy powinny koordynować swoje działania i współpracować ze sobą w zakresie wymiany informacji z dostawcami usług hostingowych na temat nakazów usunięcia oraz określania, wdrażania i oceny środków szczególnych. Taka koordynacja i współpraca są konieczne również w związku z innymi środkami mającymi na celu wykonywanie niniejszego rozporządzenia, w tym w odniesieniu do przyjmowania przepisów dotyczących kar i ich nakładania. Komisja powinna ułatwiać taką koordynację i współpracę.

(38) Ważne jest, aby właściwy organ państwa członkowskiego odpowiedzialnego za nakładanie kar był w pełni poinformowany o wydaniu nakazów usunięcia oraz o późniejszej wymianie informacji między dostawcą usług hostingowych a właściwymi organami w innych państwach członkowskich. W tym celu państwa członkowskie powinny zapewnić odpowiednie i bezpieczne kanały i mechanizmy komunikacji umożliwiające terminową wymianę istotnych informacji.

(39) Aby ułatwić szybką wymianę informacji między właściwymi organami, jak również z dostawcami usług hostingowych, oraz aby uniknąć powielania wysiłków, należy zachęcać państwa członkowskie do korzystania ze specjalnych narzędzi opracowanych przez Europol, takich jak obecna aplikacja zarządzania zgłoszeniami podejrzanych treści w internecie lub narzędzia, które ją zastąpią.

(40) Zgłoszenia dokonywane przez państwa członkowskie i Europol okazują się być skutecznym i szybkim sposobem zwiększania świadomości dostawców usług hostingowych na temat konkretnych treści dostępnych za pośrednictwem ich usług, umożliwiającym im podejmowanie szybkich działań. Takie zgłoszenia, które są mechanizmem powiadamiania dostawców usług hostingowych o informacjach, które mogłyby zostać uznane za treści o charakterze terrorystycznym, na potrzeby dobrowolnego rozważenia przez dostawcę zgodności tych treści z jego własnymi warunkami umownymi, powinny pozostać dostępne jako uzupełnienie nakazów usunięcia. Ostateczna decyzja dotycząca tego, czy usunąć treści z powodu braku zgodności z warunkami umownymi dostawcy usług hostingowych, pozostaje w jego gestii. Niniejsze rozporządzenie nie powinno mieć wpływu na mandat Europolu określony w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/794 ([11]). W związku z tym żadnego z przepisów niniejszego rozporządzenia nie należy rozumieć jako uniemożliwiającego państwom członkowskim i Europolowi wykorzystywania zgłoszeń jako instrumentu służącego do przeciwdziałania treściom o charakterze terrorystycznym w internecie.

(41) Ze względu na szczególnie poważne skutki niektórych treści o charakterze terrorystycznym w internecie dostawcy usług hostingowych powinni natychmiast informować odpowiednie organy zainteresowanego państwa członkowskiego lub właściwe organy państwa członkowskiego, w którym mają jednostkę organizacyjną lub swojego przedstawiciela prawnego, o treściach o charakterze terrorystycznym, które wiążą się z bezpośrednim zagrożeniem życia lub podejrzeniem popełnienia przestępstwa terrorystycznego. W celu zapewnienia proporcjonalności obowiązek ten powinien zostać ograniczony do przestępstw terrorystycznych zdefiniowanych w art. 3 ust. 1 dyrektywy (UE) 2017/541. Ten obowiązek informowania nie powinien oznaczać obowiązku dostawców usług hostingowych do aktywnego poszukiwania dowodów takiego bezpośredniego zagrożenia życia lub podejrzenia popełnienia przestępstwa terrorystycznego. Przez zainteresowane państwo członkowskie należy rozumieć państwo członkowskie, które ma jurysdykcję w zakresie prowadzenia postepowań przygotowawczych w sprawie tych przestępstw terrorystycznych i ich ścigania w oparciu o obywatelstwo sprawcy lub potencjalnej ofiary przestępstwa lub o miejsce będące celem aktu terrorystycznego. W przypadku wątpliwości dostawcy usług hostingowych powinni przekazywać informacje Europolowi, który powinien zapewnić odpowiednie dalsze działania zgodnie ze swoim mandatem, w tym przekazywać dalej te informacje odpowiednim organom krajowym. Właściwe organy państw członkowskich powinny być uprawnione do korzystania z takich informacji w celu podejmowania środków postępowania przygotowawczego, dostępnych na podstawie prawa Unii lub prawa krajowego.

([11]) 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).

(42) Dostawcy usług hostingowych powinni wyznaczyć lub ustanowić punkty kontaktowe w celu ułatwienia niezwłocznego zajmowania się nakazami usunięcia. Punkt kontaktowy służy jedynie celom operacyjnym. Punkt kontaktowy powinien obejmować wyspecjalizowane środki, wewnętrzne lub zlecone usługodawcom zewnętrznym, umożliwiające elektroniczne przyjmowanie nakazów usunięcia oraz środki techniczne lub kadrowe umożliwiające ich niezwłoczne przetwarzanie. Nie jest niezbędne, aby punkt kontaktowy znajdował się w Unii. Dostawca usług hostingowych powinien mieć swobodę skorzystania z istniejącego punktu kontaktowego do celów niniejszego rozporządzenia, pod warunkiem że ten punkt kontaktowy jest w stanie wykonywać zadania przewidziane w niniejszym rozporządzeniu. W celu zapewnienia usuwania treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich w ciągu jednej godziny od otrzymania nakazu usunięcia, punkt kontaktowy dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym powinien być nieustannie dostępny. Informacje na temat punktu kontaktowego powinny zawierać informacje o języku, w którym można się do niego zwracać. Aby ułatwić komunikację między dostawcami usług hostingowych a właściwymi organami, dostawców usług hostingowych zachęca się do umożliwienia komunikacji w jednym z języków urzędowych instytucji Unii, w którym dostępne są ich warunki umowne.

(43) Z braku ogólnego wymogu, by dostawcy usług hostingowych zapewniali fizyczną obecność na terytorium Unii, należy zapewnić, aby było jasne, któremu państwu członkowskiemu przysługuje jurysdykcja w stosunku do dostawcy usług hostingowych oferującego usługi w Unii. Co do zasady dostawca usług hostingowych podlega jurysdykcji państwa członkowskiego, w którym ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę. Powyższe powinno pozostawać bez uszczerbku dla przepisów dotyczących właściwości, które ustanowiono do celów wydawania nakazów usunięcia oraz decyzji wynikających z weryfikacji nakazów usunięcia na podstawie niniejszego rozporządzenia. W przypadku dostawców usług hostingowych, którzy nie mają jednostki organizacyjnej w Unii i nie wyznaczyli przedstawiciela prawnego, jurysdykcję powinno mieć jednak każde państwo członkowskie, a tym samym możliwość nakładania kar, pod warunkiem przestrzegania zasady *ne bis in idem*.

(44) Dostawcy usług hostingowych, którzy nie mają jednostki organizacyjnej w Unii, powinni wyznaczyć na piśmie przedstawiciela prawnego w celu zapewnienia wypełniania i egzekwowania obowiązków wynikających z niniejszego rozporządzenia. Dostawcy usług hostingowych powinni móc wyznaczyć, do celów niniejszego rozporządzenia, przedstawiciela prawnego już wyznaczonego do innych celów, pod warunkiem że ten przedstawiciel prawny jest w stanie wykonywać zadania przewidziane w niniejszym rozporządzeniu. Przedstawiciel prawny powinien być uprawniony do działania w imieniu dostawcy usług hostingowych.

(45) Kary są niezbędne do zapewnienia skutecznego wykonywania niniejszego rozporządzenia przez dostawców usług hostingowych. Państwa członkowskie powinny przyjąć przepisy dotyczące kar – które mogą mieć charakter administracyjny lub karny – w tym, w stosownych przypadkach, wytyczne w sprawie nakładania kar pieniężnych. Nieprzestrzeganie przepisów w poszczególnych przypadkach może być karane przy jednoczesnym przestrzeganiu zasady *ne bis in idem* i zasady proporcjonalności oraz zapewnieniu, by kary takie odzwierciedlały systematyczne niewypełnianie obowiązków. Kary mogą mieć różną formę, w tym oficjalne ostrzeżenia w przypadku drobnych naruszeń lub kary pieniężne w przypadku poważniejszych lub systematycznych naruszeń. Szczególnie surowe kary powinno nakładać się w przypadku, gdy dostawca usług hostingowych systematycznie lub uporczywie nie wypełnia obowiązków w zakresie usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich w ciągu jednej godziny od otrzymania nakazu usunięcia. Aby zapewnić pewność prawa, w niniejszym rozporządzeniu należy określić, jakie naruszenia podlegają karom oraz okoliczności, które są istotne dla określania rodzaju i poziomu takich kar. Przy ustalaniu, czy należy nałożyć kary pieniężne, należy odpowiednio uwzględnić zasoby finansowe dostawcy usług hostingowych. Ponadto właściwy organ powinien wziąć pod uwagę, czy dostawca usług hostingowych jest przedsiębiorstwem typu *start-up* lub należy do kategorii mikro-, małych lub średnich przedsiębiorstw jak zdefiniowano w zaleceniu Komisji 2003/361/WE ([12]). Pod uwagę należy wziąć dodatkowe okoliczności, takie jak to, czy zachowanie dostawcy usług hostingowych było obiektywnie nierozważne lub naganne, lub czy naruszenie zostało popełnione w wyniku zaniedbania lub umyślnie. Państwa członkowskie powinny zapewnić, aby kary nałożone za naruszenie niniejszego rozporządzenia nie zachęcały do usuwania materiałów, które nie są treściami o charakterze terrorystycznym.

(46) Stosowanie standardowych wzorów ułatwia współpracę i wymianę informacji między właściwymi organami i dostawcami usług hostingowych, co umożliwia im szybszą i skuteczniejszą komunikację. Szczególnie ważne jest zapewnienie niezwłocznego działania po otrzymaniu nakazu usunięcia. Wzory obniżają koszty tłumaczenia i przyczyniają się do zapewnienia wyższego standardu procesu. Wzory dotyczące informacji zwrotnych umożliwiają znormalizowaną wymianę informacji i mają szczególne znaczenie w przypadku, gdy dostawcy usług hostingowych nie są w stanie wykonać nakazów usunięcia. Uwierzytelnione kanały przekazywania informacji mogą zagwarantować autentyczność nakazu usunięcia, w tym dokładność daty i godziny wysłania i otrzymania nakazu.

([12]) Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

(47) W celu umożliwienia, w razie potrzeby, szybkiej zmiany treści wzorów, które mają być stosowane do celów niniejszego rozporządzenia, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w odniesieniu do dokonywania zmian załączników 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 z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa ([13]). W szczególności, aby zapewnić równy udział w przygotowywaniu aktów delegowanych, Parlament Europejskiego i Rada 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.

(48) Państwa członkowskie powinny gromadzić informacje na temat wykonywania niniejszego rozporządzenia. Państwa członkowskie powinny móc korzystać ze sprawozdań z przejrzystości przygotowywanych przez dostawców usług hostingowych i w razie konieczności uzupełniać je bardziej szczegółowymi informacjami, takimi jak własne sprawozdania z przejrzystości przygotowywane zgodnie z niniejszym rozporządzeniem. Na potrzeby oceny wykonywania niniejszego rozporządzenia powinien zostać opracowany szczegółowy program monitorowania wyników, rezultatów i skutków niniejszego rozporządzenia.

(49) W oparciu o ustalenia i wnioski zawarte w sprawozdaniu z wdrażania oraz wyniki monitorowania Komisja powinna przeprowadzić ocenę niniejszego rozporządzenia w terminie trzech lat od dnia jego wejścia w życie. Ocena ta powinna opierać się na kryteriach skuteczności, konieczności, efektywności, proporcjonalności, adekwatności, spójności i unijnej wartości dodanej. W jej ramach należy ocenić funkcjonowanie poszczególnych środków operacyjnych i technicznych przewidzianych w niniejszym rozporządzeniu, w tym skuteczność środków mających na celu poprawę wykrywania, identyfikacji i usuwania w internecie treści o charakterze terrorystycznym, skuteczność mechanizmów zabezpieczających oraz skutki dla potencjalnie zagrożonych praw podstawowych, takich jak wolność wypowiedzi i informacji, w tym wolność i pluralizm mediów, wolność prowadzenia działalności gospodarczej, prawo do prywatności i ochrony danych osobowych. Komisja powinna również ocenić wpływ na potencjalnie zagrożone interesy osób trzecich.

(50) Ponieważ cel niniejszego rozporządzenia, a mianowicie zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego poprzez przeciwdziałanie rozpowszechnianiu w internecie treści o charakterze terrorystycznym, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na rozmiary i skutki możliwe jest jego lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodne z zasadą pomocniczości określoną w art. 5 TUE. 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 przeciwdziałania wykorzystywaniu usług hostingowych do publicznego rozpowszechniania w internecie treści o charakterze terrorystycznym, w szczególności przepisy dotyczące:

a) rozsądnych i proporcjonalnych obowiązków w zakresie staranności, których mają przestrzegać dostawcy usług hostingowych w celu przeciwdziałania publicznemu rozpowszechnianiu treści o charakterze terrorystycznym za pośrednictwem ich usług oraz zapewnienia, w razie potrzeby, niezwłocznego usuwania tych treści lub uniemożliwiania dostępu do nich;

([13]) Dz.U. L 123 z 12.5.2016, s. 1.

b) środków, które mają wdrożyć państwa członkowskie – zgodnie z prawem Unii i z zastrzeżeniem odpowiednich gwarancji w zakresie ochrony praw podstawowych, w szczególności wolności wypowiedzi i informacji w otwartym i demokratycznym społeczeństwie – w celu:

(i) identyfikowania treści o charakterze terrorystycznym oraz zapewnienia ich niezwłocznego usuwania przez dostawców usług hostingowych; oraz

(ii) ułatwienia współpracy między właściwymi organami państw członkowskich, dostawcami usług hostingowych oraz, w stosownych przypadkach, z Europolem.

2. Niniejsze rozporządzenie stosuje się do dostawców usług hostingowych oferujących usługi w Unii – niezależnie od miejsca ich głównej jednostki organizacyjnej – w zakresie, w jakim publicznie rozpowszechniają informacje.

3. Materiałów publicznie rozpowszechnianych w celach edukacyjnych, dziennikarskich, artystycznych lub badawczych lub w celach zapobiegania terroryzmowi lub zwalczania terroryzmu, w tym materiałów służących wyrażaniu polemicznych lub kontrowersyjnych poglądów w ramach debaty publicznej, nie uznaje się za treści o charakterze terrorystycznym. W drodze oceny ustala się, jaki jest rzeczywisty cel danego rozpowszechniania i czy materiały są publicznie rozpowszechniane do tych celów.

4. Niniejsze rozporządzenie nie ma wpływu na obowiązek poszanowania praw, wolności i zasad, o których mowa w art. 6 TUE, i stosuje się je bez uszczerbku dla podstawowych zasad odnoszących się do wolności wypowiedzi i informacji, w tym wolności i pluralizmu mediów.

5. Niniejsze rozporządzenie pozostaje bez uszczerbku dla dyrektyw 2000/31/WE i 2010/13/UE. W odniesieniu do audiowizualnych usług medialnych zdefiniowanych w art. 1 pkt 1 lit. a) dyrektywy 2010/13/UE pierwszeństwo ma dyrektywa 2010/13/UE.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „dostawca usług hostingowych" oznacza dostawcę usług zdefiniowanych w art. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 ([14]), polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek;

2) „dostawca treści" oznacza użytkownika, który dostarczył informacje, które są lub były przechowywane i publiczne rozpowszechnianie przez dostawcę usług hostingowych;

3) „publiczne rozpowszechnianie" oznacza udostępnianie informacji, na wniosek dostawcy treści, potencjalnie nieograniczonej liczbie osób;

4) „oferowanie usług w Unii" oznacza umożliwianie osobom fizycznym lub prawnym w co najmniej jednym państwie członkowskim korzystania z usług dostawcy usług hostingowych, którego łączy z danym państwem członkowskim istotny związek;

5) „istotny związek" oznacza związek dostawcy usług hostingowych z co najmniej jednym państwem członkowskim, wynikający z posiadania jednostki organizacyjnej w Unii albo ze szczególnych kryteriów faktycznych, takich jak:

a) posiadanie znacznej liczby użytkowników jego usług w co najmniej jednym państwie członkowskim; lub

b) kierowanie jego działalności do co najmniej jednego państwa członkowskiego;

6) „przestępstwa terrorystyczne" oznaczają przestępstwa zdefiniowane w art. 3 dyrektywy (UE) 2017/541;

([14]) Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1).

7) „treści o charakterze terrorystycznym" oznaczają materiały co najmniej jednego z poniższych rodzajów; a mianowicie materiały, które:

   a) podżegają do popełnienia jednego z przestępstw, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541, w przypadku gdy takie materiały, bezpośrednio lub pośrednio, na przykład poprzez pochwalanie aktów terrorystycznych, popierają popełnianie przestępstw terrorystycznych i tym samym stwarzają niebezpieczeństwo popełnienia jednego lub większej liczby takich przestępstw;

   b) nakłaniają osobę lub grupę osób do popełnienia lub przyczynienia się do popełnienia jednego z przestępstw, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541;

   c) nakłaniają osobę lub grupę osób do uczestniczenia w działaniach grupy terrorystycznej, w rozumieniu art. 4 lit. b) dyrektywy (UE) 2017/541;

   d) udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji, lub w zakresie innych szczególnych metod lub technik w celu popełnienia lub przyczynienia się do popełnienia jednego z przestępstw terrorystycznych, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541;

   e) stwarzają zagrożenie popełnienia jednego z przestępstw, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541;

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

9) „główna jednostka organizacyjna" oznacza siedzibę główną lub siedzibę statutową dostawcy usług hostingowych, w której wykonywane są główne funkcje finansowe i sprawowana jest kontrola operacyjna.

SEKCJA II

ŚRODKI W CELU PRZECIWDZIAŁANIA ROZPOWSZECHNIANIU W INTERNECIE TREŚCI O CHARAKTERZE TERRORYSTYCZNYM

Artykuł 3

Nakazy usunięcia

1. Właściwy organ każdego państwa członkowskiego jest uprawniony do wydania nakazu usunięcia zobowiązującego dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści terrorystycznych we wszystkich państwach członkowskich.

2. W przypadku gdy właściwy organ nie wydał uprzednio dostawcy usług hostingowych nakazu usunięcia, udziela on temu dostawcy usług hostingowych informacji o mających zastosowanie procedurach i terminach co najmniej 12 godzin przed wydaniem nakazu usunięcia.

Akapitu pierwszego nie stosuje się w należycie uzasadnionych przypadkach wyjątkowych.

3. Dostawcy usług hostingowych usuwają treści o charakterze terrorystycznym lub uniemożliwiają dostęp do treści terrorystycznych we wszystkich państwach członkowskich jak najszybciej, a w każdym razie nie później niż w ciągu jednej godziny od otrzymania nakazu usunięcia.

4. Właściwe organy wydają nakazy usunięcia przy użyciu wzoru określonego w załączniku I. Nakazy usunięcia zawierają następujące elementy:

a) dane identyfikacyjne właściwego organu wydającego nakaz usunięcia i potwierdzenie autentyczności nakazu usunięcia przez ten właściwy organ;

b) wystarczająco szczegółowe uzasadnienie wyjaśniające, dlaczego dane treści uznano za treści o charakterze terrorystycznym oraz wskazanie odpowiedniego rodzaju materiałów, o których mowa w art. 2 pkt 7;

c) dokładny ujednolicony format adresowania zasobów (adres URL) oraz, w razie potrzeby, dodatkowe informacje służące identyfikacji treści o charakterze terrorystycznym;

d) wskazanie niniejszego rozporządzenia jako podstawy prawnej nakazu usunięcia;

e) data, znacznik czasu i podpis elektroniczny właściwego organu wydającego nakaz usunięcia;

f) łatwo zrozumiałe informacje na temat środków zaskarżenia przysługujących dostawcy usług hostingowych i dostawcy treści, w tym informacje na temat środków zaskarżenia do właściwego organu, możliwości wniesienia sprawy do sądu, wraz z terminami do wniesienia środków zaskarżenia;

g) gdy jest to konieczne i proporcjonalne – decyzja o nieujawnianiu informacji o usunięciu treści o charakterze terrorystycznym lub uniemożliwieniu dostępu do nich zgodnie z art. 11 ust. 3.

5. Właściwy organ kieruje nakaz usunięcia do głównej jednostki organizacyjnej dostawcy usług hostingowych lub do jego przedstawiciela prawnego wyznaczonego zgodnie z art. 17.

Właściwy organ przekazuje nakaz usunięcia punktowi kontaktowemu, o którym mowa w art. 15 ust. 1, za pomocą środków elektronicznych dających możliwość sporządzenia pisemnego potwierdzenia na warunkach, które umożliwiają ustalenie autentyczności nadawcy, w tym podanie dokładnej daty oraz godziny wysłania i otrzymania nakazu.

6. Dostawcy usług hostingowych bez zbędnej zwłoki informują właściwy organ, przy użyciu wzoru określonego w załączniku II, o usunięciu treści o charakterze terrorystycznym lub o uniemożliwieniu dostępu do treści terrorystycznych we wszystkich państwach członkowskich, wskazując w szczególności czas tego usunięcia lub uniemożliwienia dostępu.

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, w tym z dających się obiektywnie uzasadnić przyczyn technicznych lub operacyjnych, informuje bez zbędnej zwłoki właściwy organ, który wydał nakaz usunięcia, o tych powodach, przy użyciu wzoru określonego w załączniku III.

Termin określony w ust. 3 zaczyna biec od momentu, gdy ustaną powody, o których mowa w akapicie pierwszym niniejszego ustępu.

8. Jeżeli dostawca usług hostingowych nie jest w stanie wykonać nakazu usunięcia, ponieważ zawiera on oczywiste błędy lub nie zawiera informacji wystarczających do jego wykonania, informuje o tym bez zbędnej zwłoki właściwy organ, który wydał nakaz usunięcia, zwracając się o niezbędne wyjaśnienia, przy użyciu wzoru określonego w załączniku III.

Termin określony w ust. 3 zaczyna biec od momentu, gdy dostawca usług hostingowych otrzymał niezbędne wyjaśnienia.

9. Nakaz usunięcia staje się ostateczny po upływie terminu do wniesienia środka zaskarżenia, w przypadku gdy nie został on wniesiony zgodnie z prawem krajowym albo na skutek utrzymania nakazu usunięcia w wyniku wniesienia środka zaskarżenia.

Kiedy nakaz usunięcia stanie się ostateczny, właściwy organ, który wydał nakaz usunięcia, informuje o tym właściwy organ, o którym mowa w art. 12 ust. 1 lit. c), państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę.

Artykuł 4

Procedura dotycząca transgranicznych nakazów usunięcia

1. Z zastrzeżeniem art. 3, w przypadku gdy dostawca usług hostingowych nie ma głównej jednostki organizacyjnej ani przedstawiciela prawnego w państwie członkowskim właściwego organu, który wydał nakaz usunięcia, organ ten przekazuje jednocześnie kopię nakazu usunięcia właściwemu organowi państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę.

2. W przypadku gdy dostawca usług hostingowych otrzymuje nakaz usunięcia, o którym mowa w niniejszym artykule, podejmuje środki przewidziane w art. 3 oraz podejmuje niezbędne środki, by móc przywrócić treści lub dostęp do nich, zgodnie z ust. 7 niniejszego artykułu.

3. Właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, może z własnej inicjatywy – w ciągu 72 godzin od otrzymania kopii nakazu usunięcia zgodnie z ust. 1 – dokonać weryfikacji tego nakazu, aby ustalić, czy nakaz ten nie narusza w sposób poważny lub oczywisty niniejszego rozporządzenia lub praw podstawowych i wolności gwarantowanych w Karcie.

W przypadku stwierdzenia takiego naruszenia, podejmuje w tej sprawie decyzję wraz z uzasadnieniem, w tym samym terminie.

4. Dostawcy usług hostingowych i dostawcy treści mają prawo wystąpienia – w ciągu 48 godzin od otrzymania nakazu usunięcia albo informacji, o których mowa w art. 11 ust. 2 – do właściwego organu państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, z wnioskiem wraz z uzasadnieniem o przeprowadzenie weryfikacji, o której mowa w ust. 3 akapit pierwszy niniejszego artykułu.

W ciągu 72 godzin od otrzymania wniosku właściwy organ podejmuje w wyniku przeprowadzonej weryfikacji nakazu usunięcia decyzję wraz z uzasadnieniem, przedstawiając swoje ustalenia odnośnie do tego, czy doszło do naruszenia.

5. Przed podjęciem decyzji na podstawie ust. 3 akapit drugi lub decyzji stwierdzającej naruszenie na podstawie ust. 4 akapit drugi, właściwy organ informuje właściwy organ, który wydał nakaz usunięcia, o zamiarze podjęcia decyzji i o jej powodach.

6. W przypadku gdy właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, podejmuje decyzję wraz z uzasadnieniem na podstawie ust. 3 lub 4 niniejszego artykułu, niezwłocznie powiadamia o tej decyzji właściwy organ, który wydał nakaz usunięcia, dostawcę usług hostingowych, dostawcę treści, który wystąpił o przeprowadzenie weryfikacji na podstawie ust. 4 niniejszego artykułu, oraz – zgodnie z art. 14 – Europol. Jeżeli w decyzji stwierdza się naruszenie na podstawie ust. 3 lub 4 niniejszego artykułu, nakaz usunięcia przestaje wywoływać skutki prawne.

7. Po otrzymaniu decyzji stwierdzającej naruszenie, o której powiadomiono zgodnie z ust. 6, dostawca usług hostingowych natychmiast przywraca dane treści lub dostęp do nich, bez uszczerbku dla możliwości egzekwowania swoich warunków umownych zgodnie z prawem Unii i prawem krajowym.

Artykuł 5

Środki szczególne

1. Dostawca usług hostingowych narażony na treści o charakterze terrorystycznym zgodnie z ust. 4 zamieszcza, w stosownych przypadkach, w swoich warunkach umownych oraz stosuje postanowienia mające przeciwdziałać wykorzystywaniu jego usług do publicznego rozpowszechniania treści o charakterze terrorystycznym.

Działa on przy tym z zachowaniem należytej staranności, w sposób proporcjonalny i niedyskryminacyjny, odpowiednio uwzględniając we wszystkich okolicznościach prawa podstawowe użytkowników i mając na uwadze, w szczególności, zasadnicze znaczenie wolności wypowiedzi i informacji w otwartym i demokratycznym społeczeństwie, tak aby uniknąć usuwania materiałów, które nie stanowią treści o charakterze terrorystycznym.

2. Dostawca usług hostingowych narażony na treści o charakterze terrorystycznym zgodnie z ust. 4 podejmuje środki szczególne w celu ochrony swoich usług przed publicznym rozpowszechnianiem treści o charakterze terrorystycznym.

Decyzja co do wyboru środków szczególnych pozostaje w gestii dostawcy usług hostingowych. Środki takie mogą obejmować co najmniej jeden z następujących środków:

a) odpowiednie techniczne i operacyjne środki lub zdolności, takie jak odpowiedni personel lub środki techniczne do celów identyfikowania i niezwłocznego usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich;

b) łatwo dostępne i przyjazne dla użytkownika mechanizmy umożliwiające użytkownikom zgłaszanie lub sygnalizowanie dostawcy usług hostingowych domniemanych treści o charakterze terrorystycznym;

c) inne mechanizmy zwiększające świadomość na temat dostępności treści o charakterze terrorystycznym w ramach świadczonych przez niego usług, takie jak mechanizmy służące moderowaniu użytkowników;

d) inne środki, które dostawca usług hostingowych uzna za stosowne, by przeciwdziałać dostępności treści o charakterze terrorystycznym w ramach świadczonych przez niego usług.

3. Środki szczególne muszą spełniać wszystkie następujące wymogi:

a) skutecznie zmniejszać poziom narażenia usług dostawcy usług hostingowych na treści o charakterze terrorystycznym;

b) być ukierunkowane i proporcjonalne, uwzględniając w szczególności, jak duży jest poziom narażenia usług dostawcy usług hostingowych na treści o charakterze terrorystycznym, a także zdolności techniczne i operacyjne, kondycję finansową, liczbę użytkowników usług dostawcy usług hostingowych oraz ilość dostarczanych przez nich treści;

c) być stosowane w sposób, który uwzględnia pełne poszanowanie praw i uzasadnionego interesu użytkowników, w szczególności podstawowych praw użytkowników dotyczących wolności wypowiedzi i informacji, poszanowania życia prywatnego i ochrony danych osobowych;

d) być stosowane w staranny i niedyskryminacyjny sposób.

W przypadku gdy środki szczególne wiążą się ze stosowaniem środków technicznych, wprowadza się odpowiednie i skuteczne zabezpieczenia, w szczególności poprzez nadzór i weryfikację dokonywane przez człowieka, aby zapewnić dokładność i uniknąć usuwania materiałów, które nie stanowią treści o charakterze terrorystycznym.

4. Dostawca usług hostingowych jest narażony na treści o charakterze terrorystycznym, w przypadku gdy właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę:

a) podjął decyzję, opartą na obiektywnych czynnikach, takich jak fakt otrzymania przez dostawcę co najmniej dwóch ostatecznych nakazów usunięcia w ciągu ostatnich 12 miesięcy, w której stwierdził, że dostawca usług hostingowy jest narażony na treści o charakterze terrorystycznym; oraz

b) powiadomił dostawcę usług hostingowych o decyzji, o której mowa w lit. a).

5. Po otrzymaniu decyzji, o której mowa w ust. 4, lub, w stosownych przypadkach, w ust. 6, dostawca usług hostingowych powiadamia właściwy organ o środkach szczególnych, które podjął i które zamierza podjąć w celu zapewnienia zgodności z ust. 2 i 3. Dostawca usług hostingowych dokonuje tego powiadomienia w terminie trzech miesięcy od otrzymania decyzji, a następnie raz do roku. Obowiązek ten ustaje po podjęciu przez właściwy organ decyzji, na wniosek zgodnie z ust. 7, że dostawca usług hostingowych nie jest już narażony na treści o charakterze terrorystycznym.

6. Jeżeli na podstawie dokonanego powiadomienia, o którym mowa w ust. 5, i w oparciu o, w stosownych przypadkach, inne obiektywne czynniki właściwy organ uzna, że podjęte środki szczególne nie są zgodne z wymogami ust. 2 i 3, organ ten kieruje do dostawcy usług hostingowych decyzję zobowiązującą go do podjęcia niezbędnych środków w celu zapewnienia zgodności z ust. 2 i 3.

Dostawca usług hostingowych może wybrać, jaki rodzaj środków szczególnych podejmie.

7. Dostawca usług hostingowych może w dowolnym momencie zwrócić się do właściwego organu o dokonanie przeglądu oraz, w stosownych przypadkach, o zmianę lub uchylenie decyzji, o której mowa w ust. 4 lub 6.

W terminie trzech miesięcy od otrzymania wniosku właściwy organ, w oparciu o obiektywne czynniki, podejmuje decyzję wraz z uzasadnieniem w sprawie tego wniosku i powiadamia o niej dostawcę usług hostingowych.

8. Wymóg podjęcia środków szczególnych pozostaje bez uszczerbku dla art. 15 ust. 1 dyrektywy 2000/31/WE i nie pociąga za sobą ogólnego obowiązku w zakresie nadzoru przez dostawców usług hostingowych przekazywanych lub przechowywanych przez nich informacji ani ogólnego obowiązku aktywnego poszukiwania faktów lub okoliczności wskazujących na bezprawną działalność.

Wymóg podjęcia środków szczególnych nie obejmuje obowiązku stosowania przez dostawcę usług hostingowych zautomatyzowanych narzędzi.

Artykuł 6

Zachowywanie 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 lub środków szczególnych na podstawie art. 3 lub 5, jak również związane z nimi dane, które zostały usunięte w wyniku usunięcia takich treści o charakterze terrorystycznym, które to treści i dane są konieczne do:

a) kontroli w postępowaniach administracyjnych lub sądowych lub rozpatrywania skarg na podstawie art. 10 w przypadku decyzji o usunięciu treści o charakterze terrorystycznym i związanych z nimi danych lub o uniemożliwieniu do nich dostępu; lub

b) zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia postępowań przygotowawczych 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 okres sześciu miesięcy od usunięcia lub uniemożliwienia dostępu do nich. Treści o charakterze terrorystycznym są, na wniosek właściwego organu lub sądu, zachowywane przez kolejny określony okres wyłącznie wtedy, jeżeli jest to konieczne i tak długo, jak jest to konieczne do celów trwającej kontroli w postępowaniach administracyjnych lub sądowych, o których 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 podlegały odpowiednim zabezpieczeniom technicznym i organizacyjnym.

Przedmiotowe zabezpieczenia 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, oraz zapewniają wysoki poziom ochrony odnośnych danych osobowych. W razie potrzeby dostawcy usług hostingowych dokonują przeglądu i aktualizacji tych zabezpieczeń.

SEKCJA III

ZABEZPIECZENIA I ODPOWIEDZIALNOŚĆ

Artykuł 7

Obowiązki dostawców usług hostingowych w zakresie przejrzystości

1. Dostawcy usług hostingowych określają w swoich warunkach umownych w sposób jasny swoje zasady dotyczące przeciwdziałania rozpowszechnianiu treści o charakterze terrorystycznym, w tym, w stosownych przypadkach, rzeczowe wyjaśnienie funkcjonowania środków szczególnych, w tym, w stosownych przypadkach, stosowania zautomatyzowanych narzędzi.

2. Dostawca usług hostingowych, który w danym roku kalendarzowym podjął działania mające na celu przeciwdziałanie rozpowszechnianiu treści o charakterze terrorystycznym lub został zobowiązany do podjęcia działań na podstawie niniejszego rozporządzenia, udostępnia publicznie ogólnie dostępne sprawozdanie z przejrzystości na temat tych działań za ten rok. Publikuje on to sprawozdanie przed dniem 1 marca kolejnego roku.

3. Sprawozdania z przejrzystości zawierają co najmniej następujące informacje:

a) informacje na temat środków wprowadzonych przez dostawcę usług hostingowych w związku z identyfikacją i usunięciem treści o charakterze terrorystycznym lub uniemożliwieniem dostępu do nich;

b) informacje na temat środków wprowadzonych przez dostawcę usług hostingowych w celu przeciwdziałania ponownemu pojawianiu się w internecie materiałów, które wcześniej zostały usunięte lub do których dostęp został uniemożliwiony, ponieważ zostały one uznane za treści o charakterze terrorystycznym, w szczególności w przypadkach, w których zastosowano zautomatyzowane narzędzia;

c) liczbę przypadków usunięcia treści o charakterze terrorystycznym lub przypadków uniemożliwienia dostępu do takich treści w wyniku nakazów usunięcia lub środków szczególnych oraz liczbę nakazów usunięcia, w przypadku których treści nie zostały usunięte lub dostęp do treści nie został uniemożliwiony na podstawie art. 3 ust. 7 akapit pierwszy i art. 3 ust. 8 akapit pierwszy, wraz z powodami, dla których tak się stało;

d) liczbę skarg rozpatrzonych przez dostawcę usług hostingowych zgodnie z art. 10 i ich wynik;

e) liczbę i wynik kontroli w postępowaniach administracyjnych lub sądowych wszczętych przez dostawcę usług hostingowych;

f) liczbę przypadków, w których dostawca usług hostingowych został zobowiązany do przywrócenia treści lub przywrócenia dostępu do nich w wyniku kontroli w postępowaniach administracyjnych lub sądowych;

g) liczbę przypadków, w których dostawca usług hostingowych przywrócił treści lub dostęp do nich na skutek skargi dostawcy treści.

Artykuł 8

Sprawozdania właściwych organów z przejrzystości

1. Właściwe organy publikują roczne sprawozdania z przejrzystości dotyczące ich działalności prowadzonej na podstawie niniejszego rozporządzenia. Sprawozdania te zawierają co najmniej następujące informacje dotyczące danego roku kalendarzowego:

a) liczba nakazów usunięcia wydanych na podstawie art. 3, ze wskazaniem liczby nakazów usunięcia podlegających art. 4 ust. 1 oraz liczby nakazów usunięcia zweryfikowanych na podstawie art. 4, oraz informacje dotyczące wykonania tych nakazów usunięcia przez dostawców usług hostingowych, w tym liczba przypadków, w których treści o charakterze terrorystycznym zostały usunięte lub dostęp do takich treści został uniemożliwiony oraz liczba przypadków, w których treści o charakterze terrorystycznym nie zostały usunięte ani dostęp do nich nie został uniemożliwiony;

b) liczba decyzji podjętych zgodnie z art. 5 ust. 4, 6 lub 7 i informacje dotyczące wykonania tych decyzji przez dostawców usług hostingowych, w tym opis środków szczególnych;

c) liczba przypadków, w których nakazy usunięcia i decyzje podjęte zgodnie z art. 5 ust. 4 i 6 stanowiły przedmiot kontroli w postępowaniach administracyjnych lub sądowych, i informacje na temat wyniku odpowiednich postępowań;

d) liczba decyzji nakładających kary na podstawie art. 18 oraz opis rodzaju nałożonej kary.

2. Roczne sprawozdania z przejrzystości, o których mowa w ust. 1, nie zawierają informacji, które mogłyby narazić na szwank bieżącą działalność służącą zapobieganiu przestępstwom terrorystycznym, ich wykrywaniu, prowadzeniu postępowań przygotowawczych w ich sprawie i ich ściganiu lub na interesy bezpieczeństwa narodowego.

Artykuł 9

Środki prawne

1. Dostawcy usług hostingowych, którzy otrzymali nakaz usunięcia wydany na podstawie art. 3 ust. 1 lub decyzję na podstawie art. 4 ust. 4 lub art. 5 ust. 4, 6 lub 7, mają prawo do skutecznego środka prawnego. Prawo to obejmuje prawo do zaskarżenia takiego nakazu usunięcia przed sądami państwa członkowskiego właściwego organu, który wydał dany nakaz usunięcia, oraz prawo do zaskarżenia decyzji na podstawie art. 4 ust. 4 lub art. 5 ust. 4, 6 lub 7 przed sądami państwa członkowskiego właściwego organu, który podjął daną decyzję.

2. Dostawcy treści, w przypadku gdy ich treści zostały usunięte lub dostęp do ich treści został uniemożliwiony w wyniku nakazu usunięcia, mają prawo do skutecznego środka prawnego. Prawo to obejmuje prawo do zaskarżenia nakazu usunięcia wydanego na podstawie art. 3 ust. 1 przed sądami państwa członkowskiego właściwego organu, który wydał dany nakaz usunięcia, oraz prawo do zaskarżenia decyzji na podstawie art. 4 ust. 4 przed sądami państwa członkowskiego właściwego organu, który podjął daną decyzję.

3. Państwa członkowskie wprowadzają skuteczne procedury korzystania z praw, o których mowa w niniejszym artykule.

Artykuł 10

Mechanizmy rozpatrywania skarg

1. Dostawca usług hostingowych ustanawia skuteczny i dostępny mechanizm umożliwiający dostawcom treści, w przypadku gdy ich treści zostały usunięte lub dostęp do ich treści został uniemożliwiony w wyniku środków szczególnych na podstawie art. 5, złożenie skargi dotyczącej danego usunięcia lub uniemożliwienia dostępu z żądaniem przywrócenia treści lub dostępu do nich.

2. Dostawca usług hostingowych rozpatruje bez zbędnej zwłoki wszelkie skargi, jakie otrzymał za pośrednictwem mechanizmu, o którym mowa w ust. 1, i bez zbędnej zwłoki przywraca treści lub dostęp do nich, w przypadku gdy ich usunięcie lub uniemożliwienie dostępu do nich było nieuzasadnione. Informuje on skarżącego o wyniku rozpatrzenia skargi w terminie dwóch tygodni od jej otrzymania.

W przypadku odrzucenia skargi dostawca usług hostingowych informuje skarżącego o powodach swojej decyzji.

Przywrócenie treści lub dostępu do nich nie wyklucza kontroli w postępowaniach administracyjnych lub sądowych zaskarżonej decyzji dostawcy usług hostingowych lub właściwego organu.

Artykuł 11

Informacje dla dostawców treści

1. W przypadku gdy dostawca usług hostingowych usuwa treści o charakterze terrorystycznym lub uniemożliwia dostęp do nich, udostępnia on dostawcy treści informacje na temat takiego usunięcia lub uniemożliwienia dostępu.

2. Na wniosek dostawcy treści dostawca usług hostingowych informuje go o powodach usunięcia lub uniemożliwienia dostępu oraz o jego prawach do zaskarżenia nakazu usunięcia albo udostępnia dostawcy treści kopię nakazu usunięcia.

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

Ten właściwy organ może przedłużyć ten okres o kolejnych sześć tygodni, jeżeli takie nieujawnianie pozostaje uzasadnione.

SEKCJA IV

WŁAŚCIWE ORGANY I WSPÓŁPRACA

Artykuł 12

Wyznaczenie właściwych organów

1. Każde państwo członkowskie wyznacza organ lub organy właściwe w zakresie:

a) wydawania nakazów usunięcia na podstawie art. 3;

b) weryfikowania nakazów usunięcia na podstawie art. 4;

c) nadzoru nad wdrażaniem środków szczególnych na podstawie art. 5;

d) nakładania kar na podstawie art. 18.

2. Każde państwo członkowskie zapewnia, aby w ramach właściwego organu, o którym mowa w ust. 1 lit. a), został wyznaczony lub ustanowiony punkt kontaktowy zajmujący się wnioskami o wyjaśnienie i informacje zwrotne, które dotyczą nakazów usunięcia wydanych przez ten właściwy organ.

Państwa członkowskie zapewniają, aby informacje na temat punktu kontaktowego były publicznie dostępne.

3. Do dnia 7 czerwca 2022 r. państwa członkowskie powiadamiają Komisję o właściwym organie lub właściwych organach, o których mowa w ust. 1, i o zmianach w tym zakresie. Komisja publikuje to powiadomienie oraz wszelkie jego zmiany w *Dzienniku Urzędowym Unii Europejskiej*.

4. Do dnia 7 czerwca 2022 r. Komisja tworzy internetowy rejestr zawierający wykaz właściwych organów, o których mowa w ust. 1, i punktów kontaktowych wyznaczonych lub ustanowionych na podstawie ust. 2 dla każdego właściwego organu. Komisja regularnie publikuje aktualizacje rejestru.

Artykuł 13

Właściwe organy

1. Państwa członkowskie zapewniają, aby ich właściwe organy dysponowały niezbędnymi uprawnieniami i wystarczającymi zasobami, aby osiągnąć cele i wypełnić swoje obowiązki określone w niniejszym rozporządzeniu.

2. Państwa członkowskie zapewniają, by ich właściwe organy wykonywały swoje zadania określone w niniejszym rozporządzeniu w sposób obiektywny i niedyskryminacyjny, z pełnym poszanowaniem praw podstawowych. Właściwe organy nie zwracają się o instrukcje do żadnego innego organu ani nie przyjmują od niego instrukcji w związku z wykonywaniem swoich zadań określonych w art. 12 ust. 1.

Akapit pierwszy nie wyklucza sprawowania nadzoru zgodnie z krajowym prawem konstytucyjnym.

Artykuł 14

Współpraca między dostawcami usług hostingowych, właściwymi organami oraz Europolem

1. Właściwe organy wymieniają się informacjami, koordynują swoje działania oraz współpracują ze sobą i, w stosownych przypadkach, z Europolem w odniesieniu do nakazów usunięcia, w szczególności w celu uniknięcia powielania wysiłków, a także w celu poprawy koordynacji i uniknięcia konfliktów w zakresie prowadzenia postępowań przygotowawczych w różnych państwach członkowskich.

2. Właściwe organy państw członkowskiego wymieniają informacje z właściwymi organami, o których mowa w art. 12 ust. 1 lit. c) i d), koordynują z nim działania i współpracują z nim w odniesieniu do środków szczególnych podjętych na podstawie art. 5 i kar nakładanych na podstawie art. 18. Państwa członkowskie zapewniają, by właściwe organy, o których mowa w art. 12 ust. 1 lit. c) i d), posiadały wszystkie istotne informacje.

3. Do celów ust. 1 państwa członkowskie zapewniają odpowiednie i bezpieczne kanały lub mechanizmy komunikacji umożliwiające terminową wymianę istotnych informacji.

4. W celu skutecznego wykonywania niniejszego rozporządzenia oraz unikania powielania wysiłków państwa członkowskie i dostawcy usług hostingowych mogą korzystać ze specjalnych narzędzi, w tym narzędzi ustanowionych przez Europol, w celu ułatwienia w szczególności:

a) przetwarzania nakazów usunięcia na podstawie art. 3 i związanych z nimi informacji; oraz

b) współpracy w celu określenia i wdrożenia środków szczególnych na podstawie art. 5.

5. W przypadku gdy dostawcy usług hostingowych dowiedzą się o treściach o charakterze terrorystycznym, które wiążą się z bezpośrednim zagrożeniem życia, natychmiast informują organy właściwe w zakresie prowadzenia postępowań przygotowawczych i ścigania przestępstw w zainteresowanym państwie członkowskim lub zainteresowanych państwach członkowskich. Jeżeli nie ma możliwości zidentyfikowania zainteresowanego państwa członkowskiego lub zainteresowanych państw członkowskich, dostawcy usług hostingowych powiadamiają na podstawie art. 12 ust. 2 punkt kontaktowy w państwie członkowskim, w którym mają główną jednostkę organizacyjną lub w którym ich przedstawiciel prawny ma miejsce pobytu lub siedzibę, oraz przekazują informacje dotyczące tych treści o charakterze terrorystycznym Europolowi na potrzeby odpowiednich dalszych działań.

6. Zachęca się właściwe organy do przesyłania Europolowi kopii nakazów usunięcia, umożliwiając mu w ten sposób przygotowanie sprawozdania rocznego zawierającego analizę rodzajów treści o charakterze terrorystycznym będących przedmiotem nakazów usunięcia lub uniemożliwienia dostępu do nich na podstawie niniejszego rozporządzenia.

Artykuł 15

Punkty kontaktowe dostawców usług hostingowych

1. Każdy dostawca usług hostingowych wskazuje lub ustanawia punkt kontaktowy do celów odbioru nakazów usunięcia za pomocą środków elektronicznych oraz ich niezwłocznego przetwarzania na podstawie art. 3 i 4. Dostawca usług hostingowych zapewnia, aby informacje o punkcie kontaktowym były publicznie dostępne.

2. W informacjach, o których mowa w ust. 1 niniejszego artykułu, określa się języki urzędowe instytucji Unii, zgodnie z rozporządzeniem 1/58 ([15]), w których można zwracać się do punktu kontaktowego i w których mają się odbywać dalsze wymiany informacji w związku z nakazami usunięcia na podstawie art. 3. Te języki obejmują co najmniej jeden z języków urzędowych państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę.

SEKCJA V

WDROŻENIE I EGZEKWOWANIE

Artykuł 16

Jurysdykcja

1. Państwo członkowskie, w którym znajduje się główna jednostka organizacyjna dostawcy usług hostingowych, ma jurysdykcję do celów art. 5, 18 i 21. Uznaje się, że dostawca usług hostingowych, który nie ma głównej jednostki organizacyjnej w Unii, podlega jurysdykcji państwa członkowskiego, w którym ma miejsce pobytu lub siedzibę jego przedstawiciel prawny.

2. W przypadku gdy dostawca usług hostingowych, który nie ma głównej jednostki organizacyjnej w Unii, nie wyznaczy przedstawiciela prawnego, jurysdykcję mają wszystkie państwa członkowskie.

3. Jeżeli właściwy organ państwa członkowskiego wykonuje jurysdykcję na podstawie ust. 2, informuje o tym właściwe organy wszystkich pozostałych państw członkowskich.

Artykuł 17

Przedstawiciel prawny

1. Dostawca usług hostingowych, który nie ma głównej jednostki organizacyjnej w Unii, wyznacza na piśmie osobę fizyczną lub prawną jako swojego przedstawiciela prawnego w Unii do celów odbioru, stosowania się do i wykonywania nakazów usunięcia i decyzji wydanych przez właściwe organy.

2. Dostawca usług hostingowych przekazuje swojemu przedstawicielowi prawnemu uprawnienia i zasoby niezbędne do stosowania się do tych nakazów usunięcia i decyzji oraz do współpracy z właściwymi organami.

Przedstawiciel prawny ma miejsce pobytu lub siedzibę w jednym z państw członkowskich, w których dostawca usług hostingowych oferuje swoje usługi.

3. Przedstawiciel prawny może zostać pociągnięty do odpowiedzialności z tytułu naruszeń niniejszego rozporządzenia, bez uszczerbku dla odpowiedzialności dostawcy usług hostingowych i działań prawnych przeciwko dostawcy usług hostingowych.

4. Dostawca usług hostingowych powiadamia o wyznaczeniu przedstawiciela prawnego właściwy organ, o którym mowa w art. 12 ust. 1 lit. d), państwa członkowskiego, w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę.

Dostawca usług hostingowych udostępnia publicznie informacje na temat przedstawiciela prawnego.

SEKCJA VI

PRZEPISY KOŃCOWE

Artykuł 18

Kary

1. Państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia przez dostawców usług hostingowych i podejmują wszelkie środki niezbędne do zapewnienia ich wykonania. Kary takie ograniczają się do przypadków naruszeń art. 3 ust. 3 i 6, art. 4 ust. 2 i 7, art. 5 ust. 1, 2, 3, 5 i 6, art. 6, 7, 10 i 11, art. 14 ust. 5, art. 15 ust. 1 oraz art. 17.

([15]) Rozporządzenie nr 1 w sprawie określenia systemu językowego Europejskiej Wspólnoty Gospodarczej (Dz.U. 17 z 6.10.1958, s. 385).

Kary, o których mowa w akapicie pierwszym, muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie do dnia 7 czerwca 2022 r. powiadamiają Komisję o tych przepisach i środkach, a następnie niezwłocznie powiadamiają ją o zmianach mających wpływ na te przepisy i środki.

2. Państwa członkowskie zapewniają, by właściwe organy uwzględniały przy podejmowaniu decyzji w sprawie nałożenia kary i ustalaniu rodzaju i wysokości kary 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 dostawcę usług hostingowych;

d) kondycję finansową dostawcy usług hostingowych;

e) poziom współpracy dostawcy usług hostingowych z właściwymi organami;

f) charakter i rozmiary dostawców usług hostingowych, w szczególności czy jest on mikro-, małym lub średnim przedsiębiorstwem;

g) stopień winy dostawcy usług hostingowych, z uwzględnieniem podjętych przez niego środków technicznych i organizacyjnych w celu spełnienia wymogów niniejszego rozporządzenia.

3. Państwa członkowskie zapewniają, aby systematyczne lub uporczywe niedopełnianie obowiązków wynikających z art. 3 ust. 3 podlegało karom pieniężnym w wysokości do 4 % całkowitych obrotów dostawcy usług hostingowych w poprzednim roku obrotowym.

Artykuł 19

Wymogi techniczne i zmiany załączników

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

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 20 w celu dokonywania zmian załączników, by skutecznie odpowiedzieć na ewentualną potrzebę poprawienia treści wzorów nakazów usunięcia oraz służących przekazywaniu informacji na temat niemożliwości wykonania nakazów usunięcia.

Artykuł 20

Wykonywanie przekazanych uprawnień

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

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 19, powierza się Komisji na czas nieokreślony od dnia 7 czerwca 2022 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 następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność 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 z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

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 i przesyłają Komisji do dnia 31 marca każdego roku informacje, które uzyskały od swoich właściwych organów i dostawców usług hostingowych podlegających ich jurysdykcji i które dotyczą podjętych przez te organy i dostawców zgodnie z niniejszym rozporządzeniem w poprzednim roku kalendarzowym. Informacje te obejmują:

a) liczbę wydanych nakazów usunięcia oraz liczbę przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, a także szybkość, z jaką dokonano usunięcia lub uniemożliwiono dostęp;

b) środki szczególne podjęte na podstawie art. 5, w tym liczbę przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, a także szybkość, z jaką dokonano usunięcia lub uniemożliwiono dostępu;

c) liczbę wniosków o dostęp, z którymi wystąpiły właściwe organy, w odniesieniu do treści zachowywanych przez dostawcę usług hostingowych na podstawie art. 6;

d) liczbę wszczętych procedur rozpatrywania skarg oraz działań podjętych przez dostawców usług hostingowych na podstawie art. 10;

e) liczbę wszczętych kontroli w postępowaniach administracyjnych lub sądowych oraz decyzji podjętych przez właściwy organ zgodnie z prawem krajowym.

2. Do dnia 7 czerwca 2023 r. Komisja ustala szczegółowy program monitorowania wyników, 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. Wyszczególnia 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 wykonywania

Do dnia 7 czerwca 2023 r. Komisja składa Parlamentowi Europejskiemu i Radzie sprawozdanie ze stosowania niniejszego rozporządzenia. To sprawozdanie obejmuje informacje dotyczące monitorowania na podstawie art. 21 oraz informacje wynikające z obowiązków w zakresie przejrzystości na podstawie art. 8. Państwa członkowskie przekazują Komisji informacje niezbędne do sporządzenia sprawozdania.

Artykuł 23

Ocena

Do dnia 7 czerwca 2024 r. Komisja dokonuje oceny niniejszego rozporządzenia oraz przedstawia Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące jego stosowania, obejmujące informacje na temat:

a) skuteczności funkcjonowania mechanizmów gwarancyjnych i zabezpieczających, w szczególności tych przewidzianych w art. 4 ust. 4, art. 6 ust. 3 i art. 7–11;

b) wpływu stosowania niniejszego rozporządzenia na prawa podstawowe, w szczególności na wolność wypowiedzi i informacji, poszanowanie życia prywatnego i ochronę danych osobowych; oraz

c) przyczyniania się niniejszego rozporządzenia do ochrony bezpieczeństwa publicznego.

W stosownych przypadkach sprawozdaniu towarzyszą wnioski ustawodawcze.

Państwa członkowskie przekazują Komisji informacje niezbędne do sporządzenia sprawozdania.

Komisja ocenia też konieczność i wykonalność ustanowienia europejskiej platformy ds. treści o charakterze terrorystycznym w internecie, która służyłaby ułatwianiu komunikacji i współpracy w ramach niniejszego rozporządzenia.

Artykuł 24

Wejście w życie i stosowanie

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

Niniejsze rozporządzenie stosuje się od dnia 7 czerwca 2022 r.

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

Sporządzono w Brukseli dnia 29 kwietnia 2021 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
D.M. SASSOLI	A.P. ZACARIAS
Przewodniczący	*Przewodniczący*

ZAŁĄCZNIK I

NAKAZ USUNIĘCIA

(art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784)

Na podstawie art. 3 rozporządzenia (UE) 2021/784 (zwanego dalej „rozporządzeniem") adresat niniejszego nakazu usunięcia musi usunąć treści o charakterze terrorystycznym lub uniemożliwić dostęp do treści terrorystycznych we wszystkich państwach członkowskich jak najszybciej, a w każdym razie nie później niż w ciągu jednej godziny od otrzymania nakazu usunięcia.

Na podstawie art. 6 rozporządzenia adresat musi zachować treści i związane z nimi dane, które zostały usunięte lub do których dostęp został uniemożliwiony, przez okres sześciu miesięcy lub, na wniosek właściwych organów lub sądów, przez dłuższy okres.

Na podstawie art. 15 ust. 2 rozporządzenia niniejszy nakaz usunięcia należy wysłać w jednym z języków wskazanych przez adresata.

SEKCJA A:

Państwo członkowskie właściwego organu wydającego:

.....

Uwaga: dane właściwego organu wydającego należy podać w sekcjach E i F

Adresat oraz, w stosownych przypadkach, przedstawiciel prawny:

.....

Punkt kontaktowy:

.....

Państwo członkowskie, w którym dostawca usług hostingowych ma swoją główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę:

.....

Godzina i data wydania nakazu usunięcia:

.....

Numer referencyjny nakazu usunięcia:

.....

SEKCJA B: Treści o charakterze terrorystycznym, które muszą zostać usunięte lub do których musi zostać uniemożliwiony dostęp we wszystkich państwach członkowskich jak najszybciej, a w każdym razie nie później niż w ciągu jednej godziny od otrzymania nakazu usunięcia

Adres URL i dodatkowe informacje umożliwiające identyfikację i dokładną lokalizację treści o charakterze terrorystycznym:

.....

Powody uznania materiałów za treści o charakterze terrorystycznym zgodnie z art. 2 pkt 7 rozporządzenia.

Materiały (proszę zaznaczyć właściwe pole (pola)):

☐ podżegają innych do popełniania przestępstw terrorystycznych, na przykład przez pochwalanie aktów terrorystycznych, popieranie popełniania takich przestępstw (art. 2 pkt 7 lit. a) rozporządzenia)

☐ nakłaniają innych do popełniania lub przyczynienia się do popełniania przestępstw terrorystycznych (art. 2 pkt 7 lit. b) rozporządzenia)

☐ nakłaniają innych do uczestnictwa w działaniach grupy terrorystycznej (art. 2 pkt 7 lit. c) rozporządzenia)

☐ udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji, lub w zakresie innych szczególnych metod lub technik w celu popełniania lub przyczynienia się do popełniania przestępstw terrorystycznych (art. 2 pkt 7 lit. d) rozporządzenia)

☐ stwarzają zagrożenie popełnienia jednego z przestępstw terrorystycznych (art. 2 pkt 7 lit. e) rozporządzenia)

Dodatkowe informacje dotyczące uznania materiałów za treści o charakterze terrorystycznym:

.....

.....

.....

SEKCJA C: Informowanie dostawcy treści

Uwaga (proszę zaznaczyć pole, jeżeli dotyczy):

☐ ze względów bezpieczeństwa publicznego adresat **musi powstrzymać się od informowania dostawcy treści** o usunięciu treści o charakterze terrorystycznym lub uniemożliwieniu dostępu do nich

Jeżeli pole to nie ma zastosowania, zob. sekcja G w odniesieniu do szczegółów dotyczących możliwości zaskarżenia na mocy prawa krajowego nakazu usunięcia w państwie członkowskim właściwego organu wydającego (kopia nakazu usunięcia musi zostać przekazana dostawcy treści na jego wniosek)

SEKCJA D: Informowanie właściwego organu państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę

Proszę zaznaczyć właściwe pole (pola)

☐ Państwo członkowskie, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, jest inne niż państwo członkowskie właściwego organu wydającego

☐ Kopię nakazu usunięcia przekazuje się właściwemu organowi państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę

SEKCJA E: Dane właściwego organu wydającego

Rodzaj (proszę zaznaczyć właściwe pole):

☐ sędzia, sąd lub sędzia śledczy

☐ organ ścigania

☐ inny właściwy organ → proszę wypełnić również sekcję F

Dane właściwego organu wydającego lub jego przedstawiciela potwierdzające prawdziwość i poprawność nakazu usunięcia:

Nazwa właściwego organu wydającego:

.....

Imię i nazwisko lub nazwa przedstawiciela oraz zajmowane stanowisko (tytuł i stopień):

.....

Sygnatura sprawy:

.....

Adres:

.....

Numer telefonu: (nr kierunkowy państwa) (nr kierunkowy miejscowości)

.....

Numer faksu: (nr kierunkowy państwa) (nr kierunkowy miejscowości).

.....

Adres poczty elektronicznej .....

Data .....

Pieczęć urzędowa (jeżeli jest dostępna) i podpis ([1]):

.....

([1]) Złożenie podpisu nie jest konieczne w przypadku wysyłania z wykorzystaniem uwierzytelnionych kanałów przekazywania informacji, które mogą zagwarantować autentyczność nakazu usunięcia.

SEKCJA F: Dane kontaktowe na potrzeby dalszych działań

Dane kontaktowe właściwego organu wydającego do celów przekazania informacji zwrotnych na temat godziny usunięcia treści lub uniemożliwienia dostępu do nich lub przesłania dodatkowych wyjaśnień:

.....

Dane kontaktowe właściwego organu państwa członkowskiego, w którym dostawca usług hostingowych ma swoją główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę:

.....

SEKCJA G: Informacje na temat środków zaskarżenia

Informacje na temat właściwego organu lub sądu, terminów i postępowań na potrzeby zaskarżenia nakazu usunięcia:

Właściwy organ lub sąd, przed którymi nakaz usunięcia może zostać zaskarżony:

.....

Termin zaskarżenia nakazu usunięcia (dni/miesięcy, począwszy od):

.....

Link do przepisów krajowych:

.....

ZAŁĄCZNIK II

INFORMACJE ZWROTNE PO USUNIĘCIU TREŚCI O CHARAKTERZE TERRORYSTYCZNYM LUB UNIEMOŻLIWIENIU DOSTĘPU DO NICH

(art. 3 ust. 6 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784)

SEKCJA A:

Adresat nakazu usunięcia:

.....

Właściwy organ, który wydał nakaz usunięcia:

.....

Sygnatura sprawy – właściwy organ, który wydał nakaz usunięcia:

.....

Sygnatura sprawy – adresat:

.....

Godzina i data otrzymania nakazu usunięcia:

.....

SEKCJA B: Środki podjęte zgodnie z nakazem usunięcia

(Proszę zaznaczyć właściwe pole):

☐ treści o charakterze terrorystycznym zostały usunięte

☐ dostęp do treści o charakterze terrorystycznym został uniemożliwiony we wszystkich państwach członkowskich

Godzina i data podjętych środków:

.....

SEKCJA C: Dane dotyczące adresata

Nazwa dostawcy usług hostingowych:

.....

LUB

Imię i nazwisko lub nazwa przedstawiciela prawnego dostawcy usług hostingowych:

.....

Państwo członkowskie, w którym znajduje się główna jednostka organizacyjna dostawcy usług hostingowych:

.....

LUB

Państwo członkowskie, w którym ma miejsce pobytu lub siedzibę przedstawiciel prawny dostawcy usług hostingowych:

.....

Imię i nazwisko osoby upoważnionej:

.....

Adres poczty elektronicznej punktu kontaktowego:

.....

Data:

.....

ZAŁĄCZNIK III

INFORMACJE NA TEMAT NIEMOŻLIWOŚCI WYKONANIA NAKAZU USUNIĘCIA

(art. 3 ust. 7 i 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784)

SEKCJA A:

Adresat nakazu usunięcia:

.....

Właściwy organ, który wydał nakaz usunięcia:

.....

Sygnatura sprawy – właściwy organ, który wydał nakaz usunięcia:

.....

Sygnatura sprawy – adresat:

.....

Godzina i data otrzymania nakazu usunięcia:

.....

SEKCJA B: Niewykonanie

1) Nakaz usunięcia nie może zostać wykonany w terminie z następujących powodów (proszę zaznaczyć właściwe pole (pola)):

☐ siła wyższa lub faktyczna niemożliwość, których nie można przypisać dostawcy usług hostingowych, w tym z dających się obiektywnie uzasadnić przyczyn technicznych i operacyjnych

☐ nakaz usunięcia zawiera oczywiste błędy

☐ nakaz usunięcia nie zawiera wystarczających informacji

2) Proszę podać bardziej szczegółowe informacje dotyczące powodów niewykonania:

.....

3) Jeżeli nakaz usunięcia zawiera oczywiste błędy lub nie zawiera wystarczających informacji, proszę wskazać te błędy oraz potrzebne bardziej szczegółowe informacje lub wyjaśnienia:

.....

SEKCJA C: Dane dostawcy usług hostingowych lub jego przedstawiciela prawnego

Nazwa dostawcy usług hostingowych:

.....

LUB

Imię i nazwisko/nazwa przedstawiciela prawnego dostawcy usług hostingowych:

.....

Imię i nazwisko osoby upoważnionej:

.....

Dane kontaktowe (adres poczty elektronicznej):

.....

Podpis:

.....

Godzina i data:

.....