ZALECENIA

ZALECENIE KOMISJI (UE) 2018/334

z dnia 1 marca 2018 r.

w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 292,

a także mając na uwadze, co następuje:

(1) Dostawcy internetu i usługodawcy prowadzący działalność za pośrednictwem internetu przyczyniają się znacznie do innowacji, wzrostu gospodarczego i tworzenia miejsc pracy w Unii. Wielu z tych usługodawców odgrywa zasadniczą rolę w gospodarce cyfrowej, łącząc przedsiębiorstwa i obywateli oraz ułatwiając debatę publiczną oraz dystrybucję i odbiór opartych na faktach informacji oraz opinii i pomysłów. W niektórych przypadkach ich usługi są jednak wykorzystywane przez osoby trzecie w celu prowadzenia nielegalnej działalności w internecie, na przykład rozpowszechniania informacji odnoszących się do terroryzmu, niegodziwego traktowania dzieci w celach seksualnych, nielegalnego nawoływania do nienawiści bądź naruszeń przepisów prawa ochrony konsumentów, co może podważyć zaufanie użytkowników tych usług i niekorzystnie wpłynąć na modele biznesowe przedsiębiorców. W niektórych sytuacjach usługodawcy mogą nawet odnosić pewne korzyści z takiej działalności, na przykład dzięki dostępowi do treści chronionych prawem autorskim bez zezwolenia podmiotów tych praw.

(2) Występowanie nielegalnych treści w internecie ma poważne negatywne konsekwencje dla użytkowników, pozostałych zainteresowanych obywateli i przedsiębiorstw, a także dla społeczeństwa jako całości. Dostawcy usług online – ze względu na swoją kluczową rolę oraz środki i zdolności technologiczne związane z usługami, które świadczą – mają szczególny obowiązek wobec społeczeństwa, aby przyczyniać się do zwalczania nielegalnych treści rozpowszechnianych przy wykorzystaniu świadczonych przez siebie usług.

(3) Z uwagi na to, że szybkie usuwanie nielegalnych treści lub uniemożliwianie dostępu do nich są często niezbędne w celu ograniczenia ich szerszego rozpowszechniania oraz szkód, obowiązki te oznaczają między innymi, że usługodawcy ci powinni mieć możliwość szybkiego podejmowania decyzji dotyczących możliwych działań w odniesieniu do nielegalnych treści w internecie. Obowiązki te wymagają również wprowadzenia skutecznych i odpowiednich zabezpieczeń, w szczególności w celu zapewnienia, aby usługodawcy działali z należytą starannością i w sposób proporcjonalny oraz aby nie dopuścić do niezamierzonego usunięcia treści, które nie są bezprawne.

(4) Wielu dostawców usług online uznało te obowiązki i podjęło stosowne działania z tym związane. W ujęciu zbiorowym poczyniono istotne postępy w ramach dobrowolnych porozumień różnego rodzaju, w tym Forum UE ds. Internetu w odniesieniu do treści o charakterze terrorystycznym w internecie, kodeksu postępowania dotyczącego nielegalnego nawoływania do nienawiści w internecie oraz protokołu ustaleń w sprawie sprzedaży podrabianych towarów przez internet. Niemniej jednak, mimo tych obowiązków i postępów, nielegalne treści w internecie nadal stanowią poważny problem w Unii.

(5) Rada Europejska, zaniepokojona szeregiem ataków terrorystycznych w UE i rozprzestrzenianiem propagandy terrorystycznej w internecie, na posiedzeniu w dniach 22–23 czerwca 2017 r. stwierdziła, iż „oczekuje, że branża […] opracuje nowe technologie i narzędzia usprawniające automatyczne wykrywanie treści podżegających do aktów terrorystycznych i usuwanie tych treści". W rezolucji z dnia 15 czerwca 2017 r. Parlament Europejski wezwał te platformy internetowe do „wzmocnienia środków zwalczania nielegalnych i szkodliwych treści". Wezwanie przedsiębiorstw do przyjęcia bardziej proaktywnego podejścia, jeśli chodzi o ochronę ich użytkowników przed treściami o charakterze terrorystycznym, zostało powtórzone przez ministrów państw członkowskich w ramach Forum UE ds. Internetu. W odniesieniu do praw własności intelektualnej Rada w konkluzjach z dnia 4 grudnia 2014 r. w sprawie egzekwowania takich praw wezwała Komisję, aby rozważyła wykorzystanie dostępnych narzędzi do wskazywania sprawców naruszeń praw własności intelektualnej oraz wspomagającą rolę podmiotów pośrednich w zwalczaniu naruszeń praw własności intelektualnej.

(6) W dniu 28 września 2017 r. Komisja przyjęła komunikat zawierający wytyczne dotyczące obowiązków dostawców usług online w odniesieniu do nielegalnych treści w internecie ([1]). W komunikacie tym Komisja wyjaśniła, że oceni, czy konieczne są dodatkowe działania między innymi poprzez monitorowanie postępów na podstawie dobrowolnych porozumień. Niniejsze zalecenie zostało sporządzone w następstwie wspomnianego komunikatu. Odzwierciedla ono dążenia w nim określone i nadaje im praktyczny wymiar, uwzględniając jednocześnie istotne postępy poczynione za pośrednictwem tych dobrowolnych ustaleń oraz opierając się nich.

(7) Ponadto uznano w nim, iż należy wziąć pod uwagę specyfikę zwalczania różnych rodzajów nielegalnych treści w internecie oraz konkretne rozwiązania, które mogą okazać się niezbędne, w tym za pomocą specjalnych środków prawnych. Na przykład Komisja, uznając potrzebę takich szczególnych środków prawnych, przyjęła w dniu 25 maja 2016 r. wniosek dotyczący zmiany dyrektywy Parlamentu Europejskiego i Rady 2010/13/UE ([2]) ze względu na zmianę sytuacji na rynku. Ponadto w dniu 14 września 2016 r. Komisja przyjęła również dyrektywę w sprawie praw autorskich na jednolitym rynku cyfrowym ([3]), która nakłada na niektórych usługodawców obowiązek wprowadzenia – we współpracy z podmiotami prawa autorskiego – środków w celu funkcjonowania umów zawieranych z podmiotami praw o korzystanie z ich utworów lub innych przedmiotów objętych ochroną wskazanych przez podmioty praw w toku współpracy z dostawcami usług. Niniejsze zalecenie pozostaje bez wpływu na takie środki prawne i wnioski.

(8) W dyrektywie 2000/31/WE Parlamentu Europejskiego i Rady ([4]) ustanowiono wyłączenia w dziedzinie odpowiedzialności, które są – po spełnieniu pewnych warunków – dostępne dla niektórych dostawców usług online, w tym dostawców usług hostingowych w rozumieniu art. 14 tej dyrektywy. Aby skorzystać z takiego wyłączenia, dostawcy usług hostingowych powinni podejmować działania w celu usunięcia nielegalnych informacji, które przechowują, lub uniemożliwienia dostępu do nich niezwłocznie po uzyskaniu faktycznej wiedzy o nich oraz – w odniesieniu do roszczeń odszkodowawczych – świadomości stanu faktycznego lub okoliczności, które w sposób oczywisty świadczą o bezprawności. Mogą uzyskać taką wiedzę lub świadomość między innymi dzięki przesyłanym im zawiadomieniom. Jako taka, dyrektywa 2000/31/WE stanowi podstawę do opracowania procedur usuwania nielegalnych informacji i uniemożliwiania dostępu do nich. Dyrektywa ta zapewnia również państwom członkowskim możliwość nałożenia na odnośnych usługodawców obowiązku polegającego na dochowaniu należytej staranności w odniesieniu do nielegalnych treści, które mogą przechowywać.

(9) Przy podejmowaniu działań w odniesieniu do nielegalnych treści w internecie państwa członkowskie mają obowiązek poszanowania zasady kraju pochodzenia ustanowionej w dyrektywie 2000/31/WE. W związku z tym nie mogą – z powodów wchodzących w zakres dziedziny podlegającej koordynacji, jak określono w tej dyrektywie – ograniczać swobody świadczenia usług społeczeństwa informacyjnego przez usługodawców mających siedzibę w innym państwie członkowskim, jednak z zastrzeżeniem możliwości odstępstw pod pewnymi warunkami określonymi w tej dyrektywie.

(10) Ponadto kilkoma innymi aktami prawa unijnego ustanowiono ramy prawne w odniesieniu do niektórych określonych rodzajów nielegalnych treści, które są dostępne i rozpowszechniane w internecie. W szczególności dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE ([5]) zobowiązuje państwa członkowskie do podejmowania działań mających na celu usuwanie stron internetowych zawierających lub rozpowszechniających pornografię dziecięcą oraz umożliwia tym państwom blokowanie dostępu do takich stron internetowych, z zastrzeżeniem pewnych zabezpieczeń. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 ([6]), którą należy transponować do prawa krajowego do dnia 8 września 2018 r., zawiera podobne przepisy w odniesieniu do treści internetowych publicznie nawołujących do popełnienia przestępstwa terrorystycznego. W dyrektywie tej ustanowiono również minimalne zasady dotyczące definicji przestępstwa w dziedzinie przestępstw terrorystycznych, przestępstw dotyczących grupy terrorystycznej oraz przestępstw związanych z działalnością

([1]) COM(2017) 555 final z dnia 28 września 2017 r.
([2]) 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). COM(2016) 287 final.
([3]) COM(2016) 593 final z dnia 14 września 2016 r.
([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 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.U. L 335 z 17.12.2011, s. 1).
([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).

terrorystyczną. Zgodnie z dyrektywą 2004/48/WE Parlamentu Europejskiego i Rady ([1]) właściwe organy sądowe mają możliwość wystawiania nakazów przeciwko pośrednikowi, którego usługi są wykorzystywane przez osobę trzecią do naruszania prawa własności intelektualnej.

(11) W szczególności w obliczu powyższych informacji, oprócz dobrowolnych środków stosowanych przez niektórych dostawców usług online, od przyjęcia dyrektywy 2000/31/WE niektóre państwa członkowskie przyjęły przepisy dotyczące mechanizmu zgłaszania i usuwania nielegalnych treści. Pozostałe państwa członkowskie rozważają przyjęcie takich przepisów. Mechanizmy te zasadniczo mają na celu ułatwienie zawiadamiania odnośnego dostawcy usług hostingowych o treściach, które strona zawiadamiająca uznaje za nielegalne („zawiadomienie"), w następstwie czego dostawca ten może zdecydować, czy zgadza się z taką oceną i czy pragnie usunąć te treści lub uniemożliwić dostęp do nich („działanie"). Coraz bardziej pogłębiają się różnice między takimi przepisami krajowymi. W związku z tym odnośni dostawcy usług mogą podlegać szeregowi wymogów prawnych, które są rozbieżne pod względem ich treści i zakresu stosowania.

(12) W interesie rynku wewnętrznego oraz skuteczności zwalczania nielegalnych treści w internecie, jak również aby zachować zrównoważone podejście, które ma zapewniać dyrektywa 2000/31/WE, należy ustanowić pewne podstawowe zasady, którymi państwa członkowskie i dostawcy usług w tym zakresie powinni kierować się w swych działaniach.

(13) Zasady te powinny być określone i stosowane z pełnym poszanowaniem praw podstawowych chronionych porządkiem prawnym Unii, w szczególności praw zagwarantowanych w Karcie praw podstawowych Unii Europejskiej (zwanej dalej „Kartą"). Nielegalne treści w internecie należy zwalczać za pomocą odpowiednich i solidnych zabezpieczeń, aby zapewnić ochronę poszczególnych praw podstawowych wszystkich zainteresowanych stron. Te prawa obejmują, w zależności od przypadku, wolność słowa, w tym wolność otrzymywania i przekazywania informacji, prawo do poszanowania życia prywatnego oraz do ochrony danych osobowych, jak również prawo do skutecznej ochrony sądowej użytkowników odnośnych usług. Mogą również obejmować swobodę prowadzenia działalności gospodarczej, w tym swobodę zawierania umów, prawa dostawców usług hostingowych, jak również prawa dziecka oraz prawo do ochrony mienia, w tym własności intelektualnej, prawo do godności ludzkiej oraz prawo do niedyskryminacji pewnych innych zainteresowanych stron. W szczególności podejmując decyzję o usunięciu przechowywanych treści lub uniemożliwieniu dostępu do nich, dostawcy usług hostingowych powinni należycie uwzględnić prawa podstawowe oraz uzasadniony interes użytkowników tych usług, jak również kluczową rolę, jaką ci dostawcy zazwyczaj odgrywają w ułatwianiu debaty publicznej oraz rozpowszechnianiu oraz odbieraniu i rozumieniu faktów, opinii i pomysłów zgodnie z prawem.

(14) Zgodnie z podejściem horyzontalnym, leżącym u podstaw wyłączenia w dziedzinie odpowiedzialności ustanowionego w art. 14 dyrektywy 2000/31/WE, niniejsze zalecenie należy stosować w odniesieniu do wszelkiego rodzaju treści, które nie są zgodne z przepisami unijnymi lub przepisami państw członkowskich, niezależnie od dokładnego przedmiotu lub charakteru tych przepisów. Wystarczy wziąć pod uwagę przepisy państw członkowskich, których dotyczy wspomniane świadczenie usług, w szczególności tych państw członkowskich, na których terytorium dostawca usług hostingowych ma siedzibę lub na których terytorium świadczone są odnośne usługi. Ponadto podczas wykonywania niniejszego zalecenia należy wziąć pod uwagę wagę nielegalnych treści oraz wszelkie szkody, które mogą być przez nie spowodowane, co może być ściśle związane z szybkością podejmowanych działań, oraz to, czego można racjonalnie oczekiwać od dostawców usług hostingowych, uwzględniając w stosownych przypadkach stan rozwoju i możliwe wykorzystanie technologii. Należy również uwzględnić stosowne różnice, które mogą występować w przypadku różnych rodzajów nielegalnych treści, oraz działania wymagane w celu zlikwidowania tych różnic.

(15) Dostawcy usług hostingowych odgrywają szczególnie istotną rolę w zwalczaniu nielegalnych treści w internecie, gdyż przechowują oni informacje dostarczone przez użytkowników tych usług i na ich wniosek oraz udostępniają te informacje pozostałym użytkownikom, często na dużą skalę. Niniejsze zalecenie odnosi się zatem głównie do działalności i obowiązków tych dostawców. W stosownych przypadkach zalecenia można jednak również stosować odpowiednio w odniesieniu do innych dostawców usług online, na których te treści mają wpływ. Jako że celem niniejszego zalecenia jest uwzględnienie ryzyka związanego z nielegalnymi treściami w internecie mającymi wpływ na konsumentów w Unii, dotyczy ono działalności wszystkich dostawców usług hostingowych, niezależnie od tego, czy mają oni siedzibę w Unii, czy też w państwie trzecim, o ile kierują swoją działalność do konsumentów zamieszkałych w Unii.

(16) Mechanizmy składania dostawcom usług hostingowych zawiadomień, dotyczących treści uznanych za nielegalne, są ważnym środkiem zwalczania nielegalnych treści w internecie. Takie mechanizmy mogłyby ułatwić zawiadamianie przez wszystkie podmioty i wszystkich obywateli, którzy pragną tego dokonać. W związku z tym

([1]) Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej (Dz.U. L 157 z 30.4.2004, s. 45).

mechanizmy te powinny być łatwo dostępne dla wszystkich użytkowników, a korzystanie z nich nie powinno przysparzać trudności. Dostawcy usług hostingowych powinni jednak pozostać elastyczni, na przykład jeśli chodzi o format sprawozdań lub stosowaną technologię, aby uwzględnić wydajne rozwiązania oraz uniknąć nieproporcjonalnych obciążeń dla tych dostawców.

(17) Zgodnie z orzecznictwem Trybunału Sprawiedliwości dotyczącym art. 14 dyrektywy 2000/31/WE zawiadomienia powinny być wystarczająco dokładne i odpowiednio uzasadnione, aby dostawcy usług hostingowych, którzy je otrzymują, mogli z należytą starannością podjąć świadomą decyzję w odniesieniu do skutków, jakie będzie miało zawiadomienie. Należy zatem w największym możliwym stopniu zapewnić, aby ta norma została spełniona. Fakt, czy dane zawiadomienie doprowadzi do uzyskania wiedzy lub świadomości w rozumieniu art. 14 tej dyrektywy, należy jednak oceniać, uwzględniając specyfikę poszczególnych spraw, pamiętając również o tym, że taką wiedzę lub świadomość można również uzyskać w sposób inny niż za pośrednictwem zawiadomienia.

(18) Posiadanie danych kontaktowych podmiotu przekazującego zawiadomienie nie jest co do zasady konieczne, aby dostawca usług hostingowych mógł podjąć z należytą starannością świadomą decyzję w sprawie następstw otrzymania zawiadomienia. Uzależnienie przekazania zawiadomienia od podania danych kontaktowych stanowiłoby utrudnienie stwierdzenia występowania nielegalnych treści. Zawarcie danych kontaktowych jest jednak konieczne, aby dostawca usług hostingowych mógł przekazać informację zwrotną. Podmiot przekazujący zawiadomienie powinien zatem mieć możliwość opcjonalnego podania swoich danych kontaktowych.

(19) Aby zwiększyć przejrzystość i dokładność mechanizmu zgłaszania i usuwania nielegalnych treści oraz w razie potrzeby umożliwić dochodzenie roszczeń, dostawcy usług hostingowych – jeżeli posiadają dane kontaktowe podmiotów przekazujących zawiadomienia lub dostawców treści – powinni terminowo i stosownie informować te podmioty o działaniach podjętych w ramach powyższego mechanizmu, w szczególności w odniesieniu do swoich decyzji o wnioskowanym usunięciu odnośnych treści lub uniemożliwieniu dostępu do nich. Przekazywane informacje powinny być proporcjonalne, tj. powinny odpowiadać informacjom przekazanym przez odnośne osoby w ich zawiadomieniach lub zgłoszeniach sprzeciwu, a jednocześnie umożliwiać stosowne i zróżnicowane rozwiązania, nie stanowiąc nadmiernego obciążenia dla dostawców.

(20) W celu zapewnienia przejrzystości i rzetelności oraz aby unikać niezamierzonego usuwania treści, które nie są nielegalne, dostawcy treści powinni co do zasady być informowani o decyzjach o usunięciu treści przechowywanych na ich wniosek lub uniemożliwieniu dostępu do nich, jak również powinni mieć możliwość zaskarżenia takiej decyzji za pomocą zgłoszenia sprzeciwu, aby w stosownych przypadkach możliwe było uchylenie takiej decyzji, niezależnie od tego, czy decyzję podjęto na podstawie zawiadomienia bądź zgłoszenia, czy też w następstwie proaktywnych działań dostawcy usług hostingowych.

(21) Jednak z uwagi na charakter przedmiotowych treści, cel takiej procedury zgłaszania sprzeciwu i dodatkowe obciążenie, jakie ona powoduje dla dostawców usług hostingowych, nie ma uzasadnienia, aby zalecać udostępnianie takich informacji o wspomnianej decyzji oraz o możliwości zaskarżenia decyzji, w przypadku gdy oczywiste jest, że przedmiotowe treści są nielegalne oraz wiążą się z poważnym przestępstwem związanym z zagrożeniem życia lub bezpieczeństwa osób, takim jak przestępstwa określone w dyrektywie (UE) 2017/541 oraz dyrektywie 2011/93/UE. Ponadto w niektórych przypadkach względy porządku publicznego i bezpieczeństwa publicznego, a zwłaszcza względy związane z zapobieganiem, wykrywaniem i ściganiem przestępstw oraz prowadzeniem dochodzeń, mogą uzasadniać niebezpośrednie przekazanie informacji o decyzji o usunięciu treści danemu dostawcy treści. W związku z tym, jeżeli właściwy organ złożył w tym celu wniosek ze względów porządku publicznego i bezpieczeństwa publicznego, dostawcy usług hostingowych nie powinni tego czynić przez okres, o jaki wnioskuje dany organ w związku ze wspomnianymi względami. W zakresie, w jakim wiąże się to z ograniczeniem prawa do bycia poinformowanym w odniesieniu do przetwarzania danych osobowych, przestrzegać należy odpowiednich przepisów określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 ([1]).

(22) Mechanizmy zgłaszania i usuwania nielegalnych treści nie powinny w żaden sposób wpływać na prawa stron do wszczęcia postępowania sądowego zgodnie z obowiązującym prawem, w odniesieniu do wszelkich rodzajów treści, które uważa się za treści nielegalne, lub w odniesieniu do wszelkich działań podejmowanych w tym zakresie przez dostawców usług hostingu. Istotnym uzupełnieniem postępowania sądowego mogą być mechanizmy pozasądowego rozstrzygania sporów powstałych w tym kontekście, zwłaszcza jeżeli pozwalają one na skuteczne, przystępne pod względem kosztów i szybkie rozstrzyganie takich sporów. W związku z tym należy zachęcać do pozasądowego rozstrzygania sporów, pod warunkiem że stosowne mechanizmy spełniają odpowiednie normy, zwłaszcza pod względem sprawiedliwości proceduralnej, że nienaruszone pozostaje prawo dostępu stron do sądu oraz że wyeliminowane są nadużycia.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

(23) Aby móc lepiej ocenić skuteczność mechanizmów zgłaszania i usuwania nielegalnych treści oraz innych działań dostawców usług hostingowych w odniesieniu do treści uważanych za treści nielegalne, a także zapewnić rozliczalność, należy pamiętać o przejrzystości procedur wobec opinii publicznej. W związku z powyższym dostawcy usług hostingu powinni regularnie publikować sprawozdania ze stosowania powyższych mechanizmów i innych działań; sprawozdania te powinny być wystarczająco kompletne i szczegółowe, co pozwoli na odpowiednią orientację odbiorców. Dostawcy powinni ponadto zapewnić jasność *ex ante* w odniesieniu do warunków świadczonych przez siebie usług, strategii usuwania jakichkolwiek przechowywanych przez siebie treści, w tym treści nielegalnych, lub uniemożliwiania dostępu do nich.

(24) Istotnym elementem w walce z nielegalnymi treściami w internecie, stanowiącym uzupełnienie mechanizmów zgłaszania i usuwania nielegalnych treści, mogą być proporcjonalne i szczegółowe działania podejmowane w proaktywny sposób przez dostawców usług hostingowych, bez uszczerbku dla przepisów art. 15 ust. 1 dyrektywy 2000/31/WE. W odniesieniu do tych proaktywnych działań należy wziąć pod uwagę sytuację dostawców usług hostingowych, którzy – ze względu na rozmiar lub skalę prowadzonej przez siebie działalności – mają jedynie ograniczone zasoby i wiedzę fachową, a także uwzględnić potrzebę skutecznych i odpowiednich mechanizmów zabezpieczających towarzyszących tym działaniom.

(25) W szczególności podejmowanie takich proaktywnych działań może okazać się stosowne wtedy, gdy stwierdzono już nielegalny charakter treści lub rodzaj treści jest taki, że nie ma znaczenia określenie ich kontekstu. Może to zależeć ponadto od charakteru, skali i celu planowanych działań, od rodzaju odnośnych treści, od tego, czy obecność treści została zgłoszona przez organy ścigania lub Europol, a także od tego, czy podjęto już działania w odniesieniu do danych treści ze względu na fakt, że zostały uznane za nielegalne. Jeżeli chodzi w szczególności o materiały dotyczące niegodziwego traktowania dzieci w celach seksualnych, dostawcy usług hostingowych powinni podejmować proaktywne działania, aby wykrywać takie materiały i zapobiegać ich rozpowszechnianiu, zgodnie z zobowiązaniami podjętymi w ramach światowego sojuszu przeciwko niegodziwemu traktowaniu dzieci w internecie w celach seksualnych.

(26) W związku z tym w opublikowanym dnia 28 września 2017 r. komunikacie w sprawie zwalczania nielegalnych treści w internecie Komisja przedstawiła stanowisko, że dobrowolne podejmowanie takich proaktywnych środków nie powoduje automatycznie utraty przez danego dostawcę usług hostingowych korzyści płynących z wyłączenia od odpowiedzialności, o którym mowa w art. 14 dyrektywy 2000/31/WE.

(27) Zasadnicze znaczenie ma objęcie działań służących zwalczaniu nielegalnych treści w internecie skutecznymi i odpowiednimi zabezpieczeniami, których celem jest zapewnienie, aby dostawcy usług hostingowych, określając i wprowadzając w życie swoje strategie dotyczące wszelkich przechowywanych przez siebie treści, w tym treści nielegalnych, działali z należytą starannością i w sposób proporcjonalny. Tym samym użytkownikom zagwarantowana zostanie przede wszystkim swoboda otrzymywania i przekazywania informacji w internecie zgodnie z obowiązującym prawem. W uzupełnieniu wszelkich zabezpieczeń określonych przez obowiązujące prawo, na przykład dotyczących ochrony danych osobowych, należy w stosownych przypadkach ustanowić i stosować – w odniesieniu do stosowania środków automatycznych – szczególne zabezpieczenia, zwłaszcza nadzór i weryfikację przez ludzi, co pozwoli na uniknięcie jakichkolwiek niezamierzonych i błędnych decyzji.

(28) Na etapie zwalczania nielegalnych treści w internecie należy zagwarantować płynną, skuteczną i odpowiednią współpracę między właściwymi organami i dostawcami usług hostingowych. Do takiej współpracy w pozytywny sposób może w razie potrzeby przyczynić się wsparcie Europolu, na przykład przy zwalczaniu terroryzmu, niegodziwego traktowania dzieci w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej i nagabywania dzieci. Aby taką współpracę ułatwić, państwa członkowskie i dostawcy usług hostingowych powinni wyznaczyć punkty kontaktowe, a także ustanowić procedury na potrzeby przetwarzania zawiadomień przekazywanych przez te organy, w trybie priorytetowym i przy zachowaniu odpowiedniego stopnia poufności w odniesieniu do ich dokładności, z uwzględnieniem szczególnej wiedzy fachowej posiadanej przez te organy oraz ich kompetencji. W celu skutecznego zwalczania niektórych szczególnie poważnych przestępstw, takich jak przestępstwa określone w dyrektywie (UE) 2017/541 oraz w dyrektywie 2011/93/UE, na które mogą zwrócić uwagę dostawcy usług hostingowych podczas prowadzenia swojej działalności, należy zachęcać państwa członkowskie do korzystania z przewidzianej w art. 15 ust. 2 dyrektywy 2000/31/WE możliwości wprowadzania do przepisów obowiązku powiadamiania, zgodnie z obowiązującym prawem, zwłaszcza rozporządzeniem (UE) 2016/679.

(29) W uzupełnieniu odpowiednich organów również określone osoby fizyczne lub podmioty, w tym organizacje pozarządowe i stowarzyszenia handlowe, mogą posiadać szczególną wiedzę fachową i być gotowe do przejęcia, na zasadach dobrowolności, określonej odpowiedzialności związanej ze zwalczaniem nielegalnych treści w internecie. W świetle wnoszonej przez te podmioty wartości dodanej i czasami wysokiej liczby przedmiotowych zawiadomień należy zachęcać do współpracy między takimi zaufanymi podmiotami sygnalizującymi i dostawcami usług hostingowych, zwłaszcza poprzez traktowanie realizowanych przez nich zgłoszeń w sposób

priorytetowy i z odpowiednim stopniem zaufania, jeżeli chodzi o dokładność tych zgłoszeń. Jednak w związku z ich szczególnym statusem współpraca taka powinna być otwarta jedynie dla osób fizycznych i podmiotów przestrzegających wartości, na których opiera się Unia i które określono w art. 2 Traktatu o Unii Europejskiej, spełniających pewne odpowiednie warunki, które z kolei powinny być dostępne publicznie w sposób wyraźny i obiektywny.

(30) Zwalczanie nielegalnych treści w internecie wymaga podejścia całościowego, jako że takie treści często bez trudu migrują od jednego dostawcy usług hostingowych do drugiego i wykorzystują najsłabsze ogniwa łańcucha. W związku z tym istotne znaczenie ma współpraca, obejmująca przede wszystkim realizowaną na dobrowolnych zasadach wymianę doświadczeń, rozwiązań technologicznych oraz najlepszych praktyk. Taka współpraca ma szczególne znaczenie w przypadku dostawców usług hostingowych, którzy ze względu na swoją wielkość lub zasięg działania mają jedynie ograniczone zasoby i wiedzę fachową.

(31) Terroryzm wiąże się z nielegalnym i masowym wykorzystaniem przemocy wobec obywateli oraz ich zastraszaniem. Terroryści w coraz większym stopniu korzystają z internetu, aby rozpowszechniać propagandę terrorystyczną, stosując nierzadko zaawansowane metody w celu zagwarantowania szybkiego i szerokiego rozpowszechniania treści. Poczyniono wprawdzie określone postępy, zwłaszcza w ramach Forum UE ds. Internetu, jednak utrzymuje się pilna potrzeba szybszego i skuteczniejszego reagowania na treści o charakterze terrorystycznym publikowane w internecie. Konieczne jest także, aby dostawcy usług hostingowych uczestniczący w Forum UE ds. Internetu w pełni realizowali swoje zobowiązania, jeżeli chodzi o skuteczne i kompleksowe reagowanie.

(32) W świetle szczególnego charakteru walki z treściami o charakterze terrorystycznym publikowanymi w internecie należy uzupełnić zalecenia dotyczące zwalczania nielegalnych treści w ujęciu ogólnym o szczegółowe zalecenia, które odnoszą się konkretnie do zwalczania treści o charakterze terrorystycznym. Należy przy tym oprzeć się na wysiłkach podejmowanych w ramach Forum UE ds. Internetu oraz te wysiłki skonsolidować.

(33) Uwzględniając szczególnie poważne ryzyka związane z treściami o charakterze terrorystycznym publikowanymi w internecie oraz centralną rolę, jaką dostawcy usług hostingowych odgrywają w rozpowszechnianiu takich treści, ci ostatni powinni podjąć wszelkie rozsądne działania mające na celu niedopuszczanie treści o charakterze terrorystycznym oraz w miarę możliwości zapobieganie ich hostingowi, pod warunkiem że mają oni możliwość wprowadzania i egzekwowania warunków świadczenia usług, a także z uwzględnieniem potrzeby skutecznych i stosownych zabezpieczeń, bez uszczerbku dla art. 14 dyrektywy 2000/31/WE.

(34) Działania te powinny w szczególności obejmować współpracę z odpowiednimi organami i Europolem w związku ze zgłoszeniami, które stanowią specyficzny sposób powiadamiania dostawców usług hostingowych, dostosowany do szczególnych właściwości walki z treściami o charakterze terrorystycznym. Przekazując zgłoszenie, właściwe organy i Europol powinny mieć możliwość wystąpienia z wnioskiem o usunięcie treści, którą uważają za posiadającą charakter terrorystyczny, lub uniemożliwienie dostępu do niej, albo powołując się na odpowiednie przepisy mające zastosowanie, albo na warunki świadczenia usług przez danego dostawcę usług hostingowych. Takie mechanizmy zgłaszania powinny funkcjonować w uzupełnieniu mechanizmów zawiadamiania, w tym przez zaufane podmioty sygnalizujące. Mechanizmy te mogą być również stosowane do zawiadamiania o treściach uznawanych za treści o charakterze terrorystycznym.

(35) Mając na uwadze fakt, że treści o charakterze terrorystycznym są zazwyczaj najbardziej szkodliwe w pierwszej godzinie, w której pojawiają się w internecie, a także przy uwzględnieniu szczególnej wiedzy fachowej i odpowiedzialności właściwych organów i Europolu, należy co do zasady ocenić takie zgłoszenie i – w razie konieczności – podjąć w odniesieniu do niego działania w ciągu jednej godziny.

(36) Takie działania służące zwalczaniu treści o charakterze terrorystycznym powinny również obejmować proporcjonalne i szczegółowe środki proaktywne, w tym z wykorzystaniem metod zautomatyzowanych, celem wykrywania, identyfikowania i bezzwłocznego usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich oraz celem zagwarantowania, aby treści o charakterze terrorystycznym nie pojawiały się ponownie, bez uszczerbku dla przepisów art. 15 ust. 1 dyrektywy 2000/31/WE. W odniesieniu do tej kwestii należy wziąć pod uwagę potrzebę zapewnienia odpowiednich i skutecznych zabezpieczeń, które towarzyszyłyby takim działaniom, zwłaszcza zabezpieczeń zalecanych w rozdziale II niniejszego zalecenia.

(37) Podczas zwalczania treści o charakterze terrorystycznym publikowanych w internecie ogromne znaczenie ma współpraca, zarówno między dostawcami usług hostingowych, jak i między dostawcami usług hostingowych a właściwymi organami. W osiągnięciu celu, jakim jest zapobieganie rozpowszechnianiu treści o charakterze terrorystycznym wśród różnych dostawców usług hostingowych, pomocne mogą być przede wszystkim narzędzia technologiczne, które pomagają w automatycznym wyszukiwaniu treści, takie jak „baza hashów". Należy zachęcać do takiej współpracy, a także do rozwoju, uruchamiania oraz wymiany wspomnianych narzędzi technologicznych, a w razie potrzeby do korzystania z wiedzy fachowej Europolu. Takie starania służące podejmowaniu współpracy są szczególnie ważne dla dostawców usług hostingowych, którzy – ze względu na swoją wielkość lub zakres, w jakim działają – mają ograniczone zasoby i wiedzę fachową, pomagają im bowiem w skutecznym i szybkim reagowaniu na zgłoszenia oraz podejmowaniu proaktywnych działań, zgodnie z zaleceniami.

(38) Do starań służących podejmowaniu współpracy powinno się przyłączyć jak najwięcej zainteresowanych dostawców usług hostingowych; wszyscy uczestniczący dostawcy usług hostingowych powinni pomóc w optymalizacji i maksymalizacji wykorzystania wspomnianych narzędzi. Zachęcać należy także do zawierania ustaleń roboczych między wszystkimi zainteresowanymi stronami, w tym w stosownych przypadkach również z udziałem Europolu, pod warunkiem, że takie ustalenia mogą pomóc w zapewnieniu spójnego i skutecznego podejścia oraz umożliwić wymianę istotnych doświadczeń i wiedzy fachowej.

(39) Aby zapewnić poszanowanie podstawowego prawa do ochrony osób fizycznych w zakresie przetwarzania danych osobowych, a także swobodnego przepływu takich danych, dane osobowe w ramach wszelkich działań podejmowanych na potrzeby realizacji niniejszego zalecenia należy przetwarzać zgodnie z zasadami ochrony danych, a przede wszystkim z przepisami rozporządzenia (UE) 2016/679 oraz dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 ([1]). Przetwarzanie to powinno być również monitorowane przez odpowiednie organy nadzoru.

(40) Niniejsze zalecenie nie narusza praw podstawowych oraz zasad ustanowionych w szczególności w Karcie. W szczególności niniejsze zalecenie zmierza do zapewnienia pełnego poszanowania art. 1, 7, 8, 10, 11, 16, 17, 21, 24 oraz 47 Karty.

(41) Komisja zamierza ściśle monitorować działania podejmowane w odpowiedzi na niniejsze zalecenie. W związku z tym państwa członkowskie i dostawcy usług hostingowych powinni być gotowi do przekazania Komisji, na jej wniosek, wszelkich istotnych informacji, których przekazania można od nich z rozsądnego punktu widzenia oczekiwać, w celu umożliwienia takiego monitorowania. Na podstawie uzyskanych tą drogą informacji, a także wszelkich innych dostępnych informacji, w tym sprawozdań sporządzanych na podstawie różnych dobrowolnych porozumień, Komisja oceni skutki niniejszego zalecenia oraz ustali, czy wymagane są dalsze działania, w tym przedstawienie wniosku w sprawie wiążących unijnych aktów prawnych. Z uwagi na specyfikę i pilny charakter zwalczania treści o charakterze terrorystycznym monitorowanie to i ocenę należy przeprowadzać w oparciu o szczegółowe informacje i w szczególnie szybkim tempie, w ciągu trzech miesięcy od daty publikacji niniejszego zalecenia, przy czym w odniesieniu do innych treści nielegalnych stosowne będzie przeprowadzenie ich w ciągu sześciu miesięcy od daty publikacji,

PRZYJMUJE NINIEJSZE ZALECENIE:

ROZDZIAŁ I

Cel i terminologia

1. Ze względu na treści dostarczane przez dostawców treści, przechowywane przez państwa członkowskie i dostawców usług hostingowych na wniosek tych dostawców treści, zachęca się państwa członkowskie i dostawców usług hostingowych do wprowadzania skutecznych, stosownych i proporcjonalnych działań w celu zwalczania nielegalnych treści w internecie, zgodnie z zasadami określonymi w niniejszym zaleceniu oraz w pełnej zgodności z Kartą, zwłaszcza z prawem do wolności wypowiedzi i informacji, a także z innymi obowiązującymi przepisami prawa Unii, szczególnie w odniesieniu do ochrony danych osobowych, konkurencji i handlu elektronicznego.

2. Niniejsze zalecenie opiera się na postępach poczynionych w ramach dobrowolnych porozumień zawieranych między dostawcami usług hostingowych i innymi zainteresowanymi usługodawcami, dotyczących różnych rodzajów nielegalnych treści, oraz te postępy konsoliduje. W obszarze terroryzmu opiera się ono na postępach poczynionych w ramach Forum UE ds. Internetu oraz konsoliduje te postępy.

3. Niniejsze zalecenie nie narusza praw i obowiązków państw członkowskich do podejmowania działań w odniesieniu do nielegalnych treści w internecie zgodnie z przepisami prawa Unii, w tym możliwości, jaką zgodnie ze swoimi systemami prawnymi dysponują sądy lub organy administracyjne państw członkowskich, aby zwracać się do dostawców usług hostingowych o usunięcie nielegalnych treści lub uniemożliwienie dostępu do nich. Niniejsze zalecenie nie narusza również sytuacji dostawców usług hostingowych na podstawie dyrektywy 2000/31/WE i posiadanej przez nich możliwości określania i wprowadzania w życie swoich warunków świadczenia usług zgodnie z prawem Unii oraz prawem państw członkowskich.

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

4. Na potrzeby niniejszego zalecenia stosuje się następujące pojęcia:

a) „dostawca usług hostingowych" oznacza dostawcę usług społeczeństwa informacyjnego polegających na przechowywaniu informacji dostarczonych przez odbiorcę usługi na jego wniosek, w rozumieniu art. 14 dyrektywy 2000/31/WE, niezależnie od miejsca prowadzenia przez niego działalności, co pozwala na kierowanie usług do wszystkich konsumentów zamieszkujących na terytorium Unii;

b) „nielegalne treści" oznaczają wszelkie informacje, które nie są zgodne z prawem Unii lub z prawem danego państwa członkowskiego;

c) „użytkownik" oznacza każdą osobę fizyczną lub prawną, która jest odbiorcą usług świadczonych przez dostawcę usług hostingowych;

d) „dostawca treści" oznacza każdego użytkownika, który przedłożył informacje, które są lub były przechowywane na jego wniosek przez dostawcę usług hostingowych;

e) „zawiadomienie" oznacza każdy komunikat kierowany do dostawcy usług hostingowych przez podmiot zawiadamiający w odniesieniu do treści przechowywanych przez tego dostawcę usług hostingowych, uważanych przez podmiot zawiadamiający za treści nielegalne, w którym to komunikacie znajduje się wniosek o dobrowolne usunięcie danych treści przez dostawcę usług hostingowych lub uniemożliwienie dostępu do nich;

f) „podmiot zawiadamiający" oznacza osobę fizyczną lub podmiot, który przekazał zawiadomienie dostawcy usług hostingowych;

g) „zaufany podmiot sygnalizujący" oznacza osobę fizyczną lub podmiot, który jest przez dostawcę usług hostingowych uważany za osobę fizyczną lub podmiot posiadające szczególną wiedzę fachową i odpowiedzialność w zakresie walki z nielegalnymi treściami w internecie;

h) „treści o charakterze terrorystycznym" oznaczają wszelkie informacje, których rozpowszechnianie stanowi przestępstwo wymienione w dyrektywie (UE) 2017/541 lub przestępstwo terrorystyczne określone w prawie danego państwa członkowskiego, w tym rozpowszechniania istotnych informacji wytwarzanych przez grupy terrorystyczne bądź podmioty zawarte w odpowiednich wykazach sporządzonych przez Unię lub ONZ lub informacji, których autorstwo jest tym grupom bądź podmiotom przypisywane;

i) „organy ścigania" oznaczają właściwe organy wyznaczone przez państwa członkowskie zgodnie z ich prawem krajowym, które realizują zadania polegające na egzekwowaniu prawa do celów zapobiegania przestępstwom związanym z nielegalnymi treściami w internecie, prowadzenia postępowań przygotowawczych w związku z takimi przestępstwami, wykrywania takich przestępstw i ich ścigania;

j) „właściwe organy" oznaczają właściwe organy wyznaczone przez państwa członkowskie zgodnie z ich prawem krajowym do celów wykonywania zadań obejmujących zwalczanie nielegalnych treści w internecie, w tym organy ścigania i organy administracyjne, którym powierzono egzekwowanie prawa, niezależnie od charakteru lub konkretnego przedmiotu danych przepisów prawa, mającego zastosowanie w niektórych szczególnych obszarach;

k) „zgłoszenie" oznacza każdy komunikat kierowany do dostawcy usług hostingowych przez właściwy organ lub przez Europol w odniesieniu do treści przechowywanych przez tego dostawcę usług hostingowych, uważanych przez ten organ lub przez Europol za treści nielegalne, w którym to komunikacie znajduje się wniosek o dobrowolne usunięcie danych treści przez dostawcę usług hostingowych lub uniemożliwienie dostępu do nich.

ROZDZIAŁ II

Ogólne zalecenia dotyczące wszystkich rodzajów nielegalnych treści

Składanie i przetwarzanie zawiadomień

5. Należy ustanowić przepisy regulujące mechanizm składania zgłoszeń. Mechanizmy te powinny być łatwo dostępne, przyjazne dla użytkownika i powinny pozwalać na składanie zawiadomień drogą elektroniczną.

6. Mechanizmy te powinny pozwalać na składanie zawiadomień dostatecznie precyzyjnych i odpowiednio uzasadnionych i zachęcać do składania takich zawiadomień, aby umożliwić zainteresowanemu dostawcy usług hostingowych podejmowanie świadomych i rzetelnych decyzji w odniesieniu do treści, których dotyczy zawiadomienie, zwłaszcza w odniesieniu do tego, czy daną treść należy uznać za nielegalną, czy nie oraz czy należy ją usunąć bądź uniemożliwić dostęp do niej. Mechanizmy te powinny ułatwiać składanie zawiadomień, które zawierają wyjaśnienie powodów, dla których podmiot zgłaszający uznaje treść za nielegalną, a także wyraźne określenie lokalizacji takiej treści.

7. Podmioty zawiadamiające powinny mieć możliwość podania w zawiadomieniu swoich danych kontaktowych, lecz nie należy tego od nich wymagać. Jeżeli podejmą taką decyzję, ich anonimowość wobec dostawcy treści powinna być zagwarantowana.

8. Jeżeli dane kontaktowe podmiotu zawiadamiającego są znane dostawcy usług hostingowych, dostawca usług hostingowych powinien przesłać podmiotowi zgłaszającemu poświadczenie odbioru oraz bez zbędnej zwłoki poinformować go w sposób proporcjonalny o swojej decyzji w odniesieniu do treści, której dotyczy zgłoszenie.

Informowanie dostawców treści i zgłoszenie sprzeciwu

9. Jeżeli dostawca usług hostingowych zdecyduje o usunięciu jakiejkolwiek treści, którą przechowuje, lub o uniemożliwieniu dostępu do niej, ponieważ uważa ją za treść nielegalną, niezależnie od sposobów wykorzystanych do celów wykrywania, wskazywania lub usuwania takiej treści bądź uniemożliwiania dostępu do niej, i jeżeli dane kontaktowe dostawcy treści są dostawcy usług hostingowych znane, dostawca treści powinien, bez zbędnej zwłoki, zostać poinformowany w sposób proporcjonalny o tej decyzji oraz o powodach jej podjęcia, a także o możliwości zaskarżenia tej decyzji, o której mowa w pkt 11.

10. Punkt 9 nie powinien jednak mieć zastosowania w sytuacji, gdy oczywiste jest, że przedmiotowe treści są treściami nielegalnymi i odnoszą się do poważnych przestępstw wiążących się z zagrożeniem życia lub bezpieczeństwa osób. Ponadto dostawca usług hostingowych nie powinien przekazywać informacji, o których mowa w tym punkcie, jeżeli właściwy organ o to wnioskuje ze względów porządku publicznego i bezpieczeństwa, a zwłaszcza ze względów związanych z zapobieganiem, wykrywaniem i ściganiem przestępstw oraz prowadzeniem dochodzeń, oraz przez okres, jakiego ten wniosek dotyczy.

11. Dostawcy treści powinni mieć możliwość zakwestionowania decyzji podjętej przez dostawcę usług hostingowych, o której mowa w pkt 9, w rozsądnym terminie, za pomocą sprzeciwu kierowanego do danego dostawcy usług hostingowych. Mechanizm zgłaszania takich sprzeciwów powinien być przyjazny dla użytkownika i umożliwiać składanie sprzeciwu drogą elektroniczną.

12. Należy zagwarantować, aby dostawcy usług hostingowych w należyty sposób rozpatrywali otrzymywane zgłoszenia sprzeciwu. Jeżeli zgłoszenie sprzeciwu obejmuje powody, dla których dostawca usług hostingowych może uznać, że treść, do której odnosi się zgłoszenie sprzeciwu, nie jest treścią nielegalną, powinien bez zbędnej zwłoki cofnąć swoją decyzję o usunięciu treści lub uniemożliwieniu dostępu do niej, bez uszczerbku dla możliwości określenia i wyegzekwowania warunków realizacji usług zgodnie z prawem Unii oraz prawem państw członkowskich.

13. Dostawca treści, który złożył zgłoszenie sprzeciwu, a także zainteresowany podmiot zawiadamiający – o ile zainteresowany dostawca usług hostingowych zna ich dane kontaktowe – powinni bez zbędnej zwłoki zostać poinformowani o decyzji, jaką dostawca usług hostingowych podjął w odniesieniu do przedmiotowych treści.

Pozasądowe rozstrzyganie sporów

14. Zachęca się państwa członkowskie do ułatwiania, w stosownych przypadkach, pozasądowego rozstrzygania sporów, w celu rozwiązywania sporów powiązanych z usuwaniem nielegalnych treści lub uniemożliwianiem dostępu do nich. Wszelkie mechanizmy takiego pozasądowego rozstrzygania sporów powinny być łatwo dostępne, skuteczne, przejrzyste i bezstronne i powinny gwarantować, aby rozstrzyganie przebiegało w sposób uczciwy i zgodnie z obowiązującym prawem. Próby rozwiązania sporu drogą pozasądową nie powinny mieć wpływu na dostęp zainteresowanych stron do postępowania sądowego.

15. Zachęca się dostawców usług hostingowych do tego, aby – jeżeli jest to dostępne w przedmiotowych państwach członkowskich – pozwalali na korzystanie z mechanizmów pozasądowego rozstrzygania sporów.

Przejrzystość

16. Należy zachęcać dostawców usług hostingowych do publikowania wyraźnych, prostych, łatwych do zrozumienia i dostatecznie szczegółowych wyjaśnień dotyczących ich polityki w zakresie usuwania przechowywanych przez nich treści, w tym treści uważanych za nielegalne, a także uniemożliwiania dostępu do nich.

17. Należy zachęcać dostawców usług hostingowych do publikowania w regularnych odstępach czasu, najlepiej co najmniej raz w roku, sprawozdań z ich działalności dotyczącej usuwania treści uznawanych za nielegalne oraz uniemożliwiania dostępu do nich. Sprawozdania te powinny obejmować w szczególności informacje na temat ilości i rodzaju usuniętych treści, liczby otrzymanych zawiadomień i zgłoszeń sprzeciwu oraz dane dotyczące czasu potrzebnego do podjęcia działań.

Proaktywne działania

18. Należy zachęcać dostawców usług hostingowych do podejmowania, tam gdzie jest to odpowiednie, proporcjonalnych i konkretnych proaktywnych działań w odniesieniu do nielegalnych treści. Takie proaktywne działania mogą obejmować stosowanie automatycznych mechanizmów wykrywania nielegalnych treści jedynie wtedy, gdy jest to stosowne i proporcjonalne, oraz pod warunkiem stosowania skutecznych i odpowiednich zabezpieczeń, zwłaszcza zabezpieczeń, o których mowa w pkt 19 i 20.

Zabezpieczenia

19. Należy unikać usuwania treści, które nie są treściami nielegalnymi, bez uszczerbku dla zachowania przez dostawców usług hostingowych możliwości określania i wprowadzania w życie swoich warunków świadczenia usług zgodnie z prawem Unii oraz prawem państw członkowskich. W tym celu należy wprowadzić skuteczne i odpowiednie zabezpieczenia, które pozwolą zagwarantować, aby dostawcy usług hostingowych działali w sposób należyty i proporcjonalny w odniesieniu do treści, które przechowują, zwłaszcza podczas przetwarzania zawiadomień i zgłoszeń sprzeciwu oraz podejmowania decyzji o ewentualnym usunięciu treści uznawanych za nielegalne lub uniemożliwianiu dostępu do nich.

20. Jeżeli dostawcy usług hostingowych korzystają ze zautomatyzowanych mechanizmów w odniesieniu do przechowywanych przez siebie treści, należy wprowadzić skuteczne i odpowiednie zabezpieczenia gwarantujące, aby decyzje podejmowane w sprawie takich treści, zwłaszcza decyzje o usunięciu treści uznawanych za nielegalne lub uniemożliwieniu dostępu do nich, były precyzyjne i uzasadnione. Takie zabezpieczenia powinny obejmować przede wszystkim nadzór i weryfikację przez ludzi w przypadkach, gdy jest to właściwe, oraz zawsze, gdy do ustalenia, czy treść należy uznać za nielegalną, czy też nie, wymagana jest szczegółowa ocena danego kontekstu.

Ochrona przed nadużyciami

21. Należy podjąć skuteczne i stosowne działania, aby zapobiegać składaniu w złej wierze zawiadomień lub zgłoszeń sprzeciwu i podejmowaniu działań w następstwie ich złożenia, oraz innych formom nadużyć w związku z zalecanymi środkami służącymi zwalczaniu nielegalnych treści w internecie, określonymi w niniejszym zaleceniu.

Współpraca między dostawcami usług hostingowych i państwami członkowskimi

22. Państwa członkowskie i dostawcy usług hostingowych powinni wyznaczyć punkty kontaktowe dla spraw odnoszących się do nielegalnych treści w internecie.

23. Należy określić przyspieszone procedury przetwarzania zawiadomień składanych przez właściwe organy.

24. Zachęca się państwa członkowskie do wprowadzenia prawnych zobowiązań wobec dostawców usług hostingowych, aby niezwłocznie informowały organy ścigania, na potrzeby zapobiegania, wykrywania i ścigania przestępstw oraz prowadzenia dochodzeń, o wszelkich dowodach domniemanych poważnych przestępstw związanych z zagrożeniem życia lub bezpieczeństwa osób, uzyskanych w ramach ich działalności związanej z usuwaniem nielegalnych treści lub uniemożliwianiem dostępu do nich, zgodnie z obowiązującymi wymogami prawnymi, przede wszystkim w odniesieniu do ochrony danych osobowych, w tym rozporządzeniem (UE) 2016/679.

Współpraca między dostawcami usług hostingowych i zaufanymi podmiotami sygnalizującymi

25. Należy zachęcać do współpracy między dostawcami usług hostingowych i zaufanymi podmiotami sygnalizującymi. Przede wszystkim należy określić przyspieszone procedury przetwarzania zawiadomień składanych przez zaufane podmioty sygnalizujące.

26. Należy zachęcać dostawców usług hostingowych do publikowania jasnych i obiektywnych warunków określania, które osoby fizyczne lub podmioty są przez nich uznawane za zaufane podmioty sygnalizujące.

27. Celem takich warunków powinno być zapewnienie, aby osoby fizyczne i podmioty dysponowały niezbędną wiedzą fachową i realizowały swoją działalność jako zaufane podmioty sygnalizujące w rzetelny i obiektywny sposób, w myśl wartości, na których opiera się Unia.

Współpraca między dostawcami usług hostingowych

28. Dostawcy usług hostingowych powinni, o ile to stosowne, wymieniać doświadczenia, rozwiązania technologiczne i najlepsze praktyki dotyczące zwalczania nielegalnych treści w internecie – między sobą, a przede wszystkim z udziałem dostawców usług hostingowych, którzy ze względu na swoją wielkość lub zakres, w jakim działają, dysponują ograniczonymi zasobami i wiedzą fachową, w tym w ramach bieżącej współpracy między dostawcami usług hostingowych, za pomocą kodeksów postępowania, protokołów ustaleń i innych dobrowolnych porozumień.

ROZDZIAŁ III

Szczegółowe zalecenia dotyczące treści o charakterze terrorystycznym

Zalecenia ogólne

29. Szczegółowe zalecenia dotyczące treści o charakterze terrorystycznym określone w niniejszym rozdziale mają zastosowanie w uzupełnieniu zaleceń ogólnych określonych w rozdziale II.

30. Dostawcy usług hostingowych powinni wyraźnie określić w swoich regulaminach, iż nie będą przechowywać treści o charakterze terrorystycznym.

31. Dostawcy usług hostingowych powinni wprowadzić środki uniemożliwiające im przechowywanie treści o charakterze terrorystycznym, przede wszystkim chodzi tu o zgłoszenia, działania proaktywne oraz współpracę zgodnie z pkt 32–40.

Składanie i przetwarzanie zgłoszeń

32. Państwa członkowskie powinny zapewnić, aby ich właściwe orany dysponowały potencjałem i odpowiednimi zasobami na potrzeby skutecznego wykrywania i identyfikowania treści o charakterze terrorystycznym oraz przekazywania zgłoszeń zainteresowanym dostawcom usług hostingowych, zwłaszcza za pośrednictwem krajowych jednostek ds. zgłaszania podejrzanych treści w internecie oraz we współpracy z unijną jednostką ds. zgłaszania podejrzanych treści w internecie przy Europolu.

33. Należy określić mechanizmy umożliwiające przekazywanie zgłoszeń. Należy ustanowić przyspieszone procedury rozpatrywania zgłoszeń, zwłaszcza zgłoszeń przekazywanych przez krajowe jednostki ds. zgłaszania podejrzanych treści w internecie oraz unijną jednostkę ds. zgłaszania podejrzanych treści w internecie przy Europolu.

34. Dostawcy usług hostingowych powinni bez zbędnej zwłoki przesyłać potwierdzenia otrzymania zgłoszeń i informować właściwy organ lub Europol o swoich decyzjach w odniesieniu do treści, do których odnoszą się zgłoszenia, wskazując przy tym, w zależności od przypadku, czy usunięto treść lub uniemożliwiono dostęp do niej, czy też podjęto decyzję o nieusuwaniu treści oraz nieuniemożliwianiu dostępu do niej.

35. Dostawcy usług hostingowych powinni dokonywać oceny i, w stosownych przypadkach, co do zasady usuwać treść określoną w zgłoszeniu lub uniemożliwiać dostęp do niej w ciągu jednej godziny od chwili otrzymania zgłoszenia.

Proaktywne działania

36. Dostawcy usług hostingowych powinni podejmować proporcjonalne i szczegółowe działania proaktywne, w tym z wykorzystaniem zautomatyzowanych metod, w celu wykrywania, wskazywania i bezzwłocznego usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich.

37. Dostawcy usług hostingowych powinni podejmować proporcjonalne i szczegółowe działania proaktywne, w tym z wykorzystaniem zautomatyzowanych metod, aby bezzwłocznie uniemożliwiać dostawcom treści ponowne zamieszczanie treści, która została właśnie usunięta lub do której właśnie uniemożliwiono dostęp ze względu na fakt, że jest to treść o charakterze terrorystycznym.

Współpraca

38. W celu uniemożliwiania rozpowszechniania treści o charakterze terrorystycznym wśród różnych usług hostingowych należy zachęcać dostawców usług hostingowych do współpracy za pośrednictwem wymiany i optymalizacji skutecznych, stosownych i proporcjonalnych narzędzi technologicznych, w tym narzędzi pozwalających na automatyczne wykrywanie treści. Tam, gdzie jest to możliwe z technologicznego punktu widzenia, należy przejmować wszystkie odpowiednie formaty, za pośrednictwem których rozpowszechniane są treści o charakterze terrorystycznym. Taka współpraca powinna w szczególności obejmować dostawców usług hostingowych, którzy ze względu na swoją wielkość lub zasięg działania mają ograniczone zasoby i wiedzę fachową.

39. Należy zachęcać dostawców usług hostingowych do podejmowania działań niezbędnych do właściwego funkcjonowania i doskonalenia narzędzi, o których mowa w pkt 38, zwłaszcza poprzez udostępnianie narzędzi identyfikujących wszelkie treści uznawane za treści o charakterze terrorystycznym, oraz pełne wykorzystywanie możliwości stwarzanych przez te narzędzia.

40. Właściwe organy i dostawcy usług hostingowych powinni zawierać ustalenia robocze, w stosownych przypadkach również z Europolem, dotyczące kwestii odnoszących się do treści o charakterze terrorystycznym w internecie, udoskonalając mechanizmy zgłaszania, zapobiegając zbędnemu powielaniu starań oraz przyspieszając dokonywanie zgłoszeń przez organy ścigania na potrzeby dochodzeń związanych z terroryzmem.

ROZDZIAŁ IV

Zapewnianie informacji

41. Państwa członkowskie powinny w regularnych odstępach czasu, a najlepiej co trzy miesiące, przedstawiać Komisji sprawozdania w sprawie zgłoszeń przekazywanych przez właściwe organy oraz decyzji podejmowanych przez dostawców usług hostingowych w odpowiedzi na te zgłoszenia, jak również w sprawie ich współpracy z dostawcami usług hostingowych w związku ze zwalczaniem treści o charakterze terrorystycznym.

42. Aby umożliwić monitorowanie skuteczności niniejszego zalecenia w odniesieniu do treści o charakterze terrorystycznym, najpóźniej trzy miesiące od daty jego publikacji, dostawcy usług hostingowych powinni udostępnić Komisji, na jej wniosek, wszelkie informacje pozwalające na takie monitorowanie. Informacje te mogą w szczególności obejmować informacje o ilości treści, które zostały usunięte lub do których uniemożliwiono dostęp, czy to w następstwie zgłoszeń, zawiadomień czy też podejmowania proaktywnych działań i stosowania zautomatyzowanych metod. Mogą one obejmować również liczbę otrzymanych zgłoszeń oraz czas potrzebny do podjęcia działań, a także ilość treści, w przypadku których udało się zapobiec ich dostarczeniu lub ponownemu dostarczeniu, dzięki zastosowaniu zautomatyzowanego wykrywania treści oraz innych narzędzi technologicznych.

43. Aby umożliwić monitorowanie oddziaływania niniejszego zalecenia w odniesieniu do treści nielegalnych, innych niż treści o charakterze terrorystycznym, najpóźniej sześć miesięcy od daty jego publikacji państwa członkowskie i dostawcy usług hostingowych powinni udostępnić Komisji, na jej wniosek, wszelkie informacje pozwalające na takie monitorowanie.

Sporządzono w Brukseli dnia 1 marca 2018 r.

W imieniu Komisji
Andrus ANSIP
Wiceprzewodniczący