



Warszawa, 6 listopada 2018 r.

**Stanowisko Fundacji Panoptykon¹
w sprawie projektu rozporządzenia w sprawie zapobiegania rozpowszechnianiu w
Internecie treści o charakterze terrorystycznym²**

I. Wstęp

Przed omówieniem szczegółowych zagadnień związanych z projektem Rozporządzenia Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym (dalej: **projekt**) chcemy poddać w wątpliwość, czy ta regulacja jest w ogóle potrzebna. Jak zwraca uwagę EDRI³, 146-stronicowa ocena wpływu dołączona do projektu opiera się na nieporozumieniach i błędnych wnioskach z konsultacji publicznych. Na brak oparcia projektu na pogłębionej analizie wskazuje chociażby brak wyliczeń dotyczących kosztów wdrożenia wymaganych projektem rozwiązań przez hostingodawców.

Jednocześnie zwracamy uwagę, że dyrektywa Parlamentu Europejskiego i Rady UE 2017/541 z 15 marca 2017 r. w sprawie zwalczania terroryzmu umożliwia Państwom Członkowskim podjęcie działań mających na celu usuwanie treści internetowych nawołujących do popełnienia przestępstwa terrorystycznego (por. art. 21). Jednocześnie Komisja Europejska, zgodnie z art. 29 dyrektywy, zobowiązana jest do przedstawienia Parlamentowi i Radzie sprawozdania, w którym oceni działanie dyrektywy, w tym jej wpływ na prawa podstawowe (por. art. 29). Naszym zdaniem, dopiero na podstawie oceny funkcjonowania przepisów przyjętych na podstawie dyrektywy Komisja Europejska powinna podejmować decyzję o ewentualnych dalszych działaniach w sprawie zapobiegania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym. Tymczasem zamiast oprzeć swoją decyzję na analizie funkcjonowania dotychczasowych rozwiązań, Komisja podejmuje nową inicjatywę legislacyjną. W obliczu zbliżających się wielkimi krokami wyborów do Parlamentu Europejskiego, które zaplanowane są na maj 2019 r., działanie to sprawia wrażenie nastawionego przede wszystkim na cel o charakterze politycznym, a nie na rozwiązanie konkretnych problemów.

Abstrahując jednak od wątpliwości dotyczących konieczności przyjmowania zaproponowanych rozwiązań, przedstawiamy poniżej naszą analizę dotyczącą części z nich. W pkt II przedstawiamy uwagi dotyczące definicji treści o charakterze terrorystycznym, w pkt III – dotyczące planowanych środków w celu zapobiegania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym, w pkt IV – dotyczące przejrzystości i monitorowania.

¹ Stanowisko przygotowane przez Dorotę Głowacką oraz Wojciecha Klickiego,

² Projekt z dnia 4 lipca 2018 r.

³ EU's flawed arguments on terrorist content give big tech more power, <https://edri.org/eus-flawed-arguments-on-terrorist-content-give-big-tech-more-power/>

II. Treści o charakterze terrorystycznym

Przed przejściem do omówienia zaproponowanych metod zapobiegania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym zwracamy uwagę na samą definicję tych treści. Zgodnie z art. 2 pkt 5 projektu jest to m.in. *zachęcanie do przyczyniania się do przestępstw terrorystycznych lub propagowanie działalności grupy terrorystycznej, w szczególności poprzez zachęcanie do udziału w grupie terrorystycznej*. Definicją treści o charakterze terrorystycznym objęte jest również podżeganie i propagowanie (w tym poprzez gloryfikowanie) przestępstw o charakterze terrorystycznym.

Uważamy, że projekt zdecydowanie zbyt szeroko zakreśla katalog treści, które mogą zostać zablokowane lub usunięte. Szczególnie istotny jest brak kryterium zagrożenia wiążącego się z dostępnością określonej treści.

Zarówno w proponowanych definicjach (art. 2), jak i kolejnych przepisach nie znalazło się zastrzeżenie, że blokadą będą obejmowane jedynie te treści, których dalsze rozpowszechnianie stanowić będzie realne zagrożenie dla bezpieczeństwa. Zarówno w trybie przewidzianym artykułem 4 (nakaz usunięcia), jak i art. 5 (zgłoszenia) ocena taka nie następuje na żadnym etapie.

Tymczasem cytowana wyżej definicja treści o charakterze terrorystycznym ma niezwykle ogólny charakter i pozwala uznać za taką treść np.:

- wypowiedź w dyskusji na portalu społecznościowym wyrażającą aprobatę dla popełnionego przestępstwa o charakterze terrorystycznym;
- wypowiedź o charakterze ironicznym czy żartobliwym;
- wypowiedź niegenerującą żadnego konkretnego zagrożenia (np. ze względu na swoją ogólność);
- wypowiedź dotyczącą zdarzeń o charakterze historycznym wypełniających znamiona przestępstw o charakterze terrorystycznym.

W naszej ocenie środki ograniczające wolność słowa muszą być adekwatne do realnych zagrożeń wiążących się z „podejrzaną” treścią, tymczasem projekt rozporządzenie nie zawiera elementu oceny realnego zagrożenia wiążącego się z konkretną treścią. Zdajemy sobie co prawda sprawę z deklaracji zawartej w motywie 7 projektu, zgodnie z którym właściwe organy powinny przyjmować wyłącznie środki, które są konieczne, odpowiednie i proporcjonalne w ramach społeczeństwa demokratycznego, niemniej aby to ograniczenie miało praktyczną wartość, powinno zostać doprecyzowane w konkretnym przepisie.

Jednak przede wszystkim szeroki i nieprecyzyjny charakter definicji treści o charakterze terrorystycznym potęguje zagrożenia dla wolności słowa wynikające z tzw. *over-blockingu*, czyli nadmiernego ograniczania dostępu do treści.

III. Planowane środki w celu zapobiegania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym

W tej części stanowiska odnosimy się do relacji pomiędzy dwoma trybami zapobiegania rozpowszechnianiu treści (pkt 1), procedury zgłaszania treści (pkt 2), procedury nakazywania usunięcia treści (pkt 3) i proaktywnych środków (pkt 4).

1. Bezzasadność wprowadzenia dwóch trybów usuwania treści

Projekt rozporządzenia przewiduje wprowadzenie dwóch „trybów” usuwania lub blokowania „treści o charakterze terrorystycznym”. W pierwszym dostawcy usług hostingowych mają być zobligowani do usuwania bądź blokowania treści na mocy decyzji określonego organu publicznego uprawnionego do wydania tzw. nakazu usunięcia (art. 4). W drugim, dostawcy będą zobowiązani do reagowania na niewiążące „zgłoszenia” dotyczące danej treści o charakterze terrorystycznym skierowane przez organy publiczne uprawnione do wykrywania i identyfikacji takich treści, a także odpowiednie organy UE (art. 5). W drugim przypadku decyzja o usunięciu/zablokowaniu danego materiału będzie należała do dostawców usług hostingowych i ma być podejmowana zgodnie z postanowieniami wewnętrznych regulaminów tych podmiotów. Jednocześnie dostawcy usług hostingowych będą zobligowani do poinformowania uprawnionego organu, który wystosował zgłoszenie, o podjętych działaniach.

Wprowadzenie wskazanych wyżej dwóch ścieżek usuwania bądź blokowania treści o charakterze terrorystycznym budzi poważne wątpliwości.

• Arbitralność wyboru ścieżki działania

Zgodnie z art. 4 ust. 1 przedmiotem decyzji o usunięciu lub blokadzie mają być treści o charakterze terrorystycznym. Z kolei zgodnie z art. 5 ust. 4 zgłoszenie zawiera powody, „dla których treści uważa się za treści o charakterze terrorystycznym”. Oznacza to, że ta sama treść może stać się przedmiotem zarówno procedury opisanej w art. 4, jak i procedury opisanej w art. 5. Rozwiązanie to stwarza ryzyko arbitralnej decyzji organów państwa, z której ścieżki skorzystać – obwarowanego pewnymi gwarancjami „trybu wiążącego” (art. 4) czy pozostawiającego znacznie większą swobodę podmiotowi wnioskującemu „trybu niewiążącego” (art. 5).

2. Krytyka trybu „zgłoszenia” (art. 5)

Poza brakiem kryteriów rozstrzygających, kiedy zastosowana będzie procedura nakazu usunięcia, a kiedy zgłoszenia, ta druga budzi szereg innych poważnych wątpliwości.

• Hostingodawcy w roli arbitrów

O ile w przypadku „trybu wiążącego” projekt rozporządzenia wprowadza możliwość zakwestionowania i zweryfikowania decyzji uprawnionego organu w ramach krajowej procedury odwoławczej (czyli np. przed sądem wyższej instancji), o tyle w przypadku skierowania niewiążącego zgłoszenia, organ zgłaszający „jedynie” sygnalizuje szkodliwą treść dostawcy usług hostingowych, nie ponosząc żadnej odpowiedzialności za podjęte na skutek zgłoszenia działania. W „trybie niewiążącym” ciężar oceny charakteru zgłoszonej treści oraz odpowiedzialność za decyzję o jej zablokowaniu czy usunięciu zostają przeniesione w pełni na dostawców usług hostingowych. Projekt rozporządzenia stawia zatem hostingodawców w roli arbitrów rozstrzygających ostatecznie o dopuszczalności danej treści w sieci, pomimo, że podmioty te mają znacznie bardziej ograniczone kompetencje do rzetelnej analizy zgłaszanych materiałów. Stanowi to przejaw prywatyzacji walki z terroryzmem, która to walka należy do zadań państwa i odpowiedzialność za nią nie powinna być w żadnej mierze delegowana na podmioty prywatne.

• Presja zamiast decyzji organów państwa

Ponadto zaproponowany mechanizm otwiera drogę do wywierania „miękkiej” presji przez organy państwa w stosunku do dostawców usług hostingowych, powodując że w praktyce podmioty te będą traktować otrzymane „sugestie” jako silny impuls do zablokowania treści (tym bardziej, że oceny zgłoszonych treści mają dokonywać „priorytetowo” oraz informować następnie o podjętych

działaniach organ zgłaszający⁴. Procedura niewiążącego zgłaszania treści może być wykorzystywana przez organy państwa jako „wygodniejsza” (ponieważ nieobwarowana gwarancjami chroniącymi prawa użytkowników sieci) metoda eliminowania określonych treści z obiegu informacyjnego w cyberprzestrzeni. Organy uprawnione będą mogły bowiem zgłaszać hostingodawcom kontestowane treści z pominięciem wymogów proceduralnych przewidzianych dla „trybu wiążącego” oraz bez ryzyka, że zostaną rozliczone z prawidłowości takiego działania. W skrajnej sytuacji można sobie wręcz wyobrazić scenariusz, w którym tryb ten, pod pretekstem walki z treściami o charakterze terrorystycznymi, będzie nadużywany przez organy państwa do ograniczania dostępności w Internecie innych niepożądanych materiałów, np. wypowiedzi krytycznych wobec władzy publicznej.

- **Prywatyzacja kontroli nad przepływem treści w sieci**

Państwo, stosując „niewiążący tryb” blokowania treści o charakterze terrorystycznym, zrzeka się kontroli nad tym obszarem, oddając go w ręce prywatnych podmiotów, które w swojej działalności kierują się przede wszystkim interesem ekonomicznym. Podmioty te podejmują decyzje dotyczące dostępności treści w oparciu o wewnętrzne regulacje, a nie przepisy obowiązującego prawa, często w sposób arbitralny i nieprzejrzysty, kosztem należytego poszanowania praw użytkowników.

- **Brak gwarancji proceduralnych**

Dodatkowo w zaproponowanym rozporządzeniu nie wprowadzono kluczowego mechanizmu zabezpieczającego użytkowników przed nadużywaniem „władzy” powierzonej dostawcom usług internetowych, tj. niezależnej, zewnętrznej kontroli nad decyzjami o zablokowaniu/usunięciu treści, pozwalającej na ich skuteczne zakwestionowanie dostawcom treści (jest jedynie mowa o konieczności wprowadzenia przez firmy internetowe wewnętrznej procedury odwoławczej). W efekcie „niewiążący tryb” może sprzyjać nadmiernemu usuwaniu/blokowaniu treści zgodnych z prawem (w tym treści mających istotne publiczne znaczenie), które powinny być uprawnione w debacie publicznej.

Warto w tym kontekście podkreślić, że zaproponowany model niewiążącego sygnalizowania treści o charakterze terrorystycznym nie odpowiada międzynarodowym standardom swobody wypowiedzi wypracowanym przez organizacje i instytucje międzynarodowe zajmujące się ochroną praw człowieka. W Rekomendacji CM/Rec(2018)2⁵ Komitet Ministrów Rady Europy zwraca uwagę że wszelkie wnioski, żądania lub inne działania władz publicznych skierowane do hostingodawców, które ingerują w prawa człowieka i podstawowe wolności, prowadząc np. do zablokowania treści w Internecie, powinny mieć odpowiednią podstawę prawną, realizować uprawniony cel oraz stanowić środek niezbędny i proporcjonalny w demokratycznym społeczeństwie zgodnie z art. 10 Europejskiej Konwencji Praw Człowieka. W szczególności państwa nie mogą wywierać nacisku na dostawców usług hostingowych w kwestii blokowania/usuwania treści przy użyciu środków „pozaprawnych” oraz nie powinny co do

⁴ Więcej o zagrożeniach związanych z wywieraniem „miękkiej” lub nieformalnej presji na hostingodawców przez władze państwowe i związanymi z tym zjawiskiem zagrożeniami dla swobody wypowiedzi: Patrick Leerssen, *Cut Out By The Middle Man: The Free Speech Implications Of Social Network Blocking and Banning In The EU*, 6 (2015) JIPITEC 99 para 1., <https://www.jipitec.eu/issues/jipitec-6-2-2015/4271>.

⁵ Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, 7 marca 2018, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14.

zasady domagać się tego w innym trybie niż w drodze podlegającej zaskarżeniu decyzji wydanej przez sąd bądź inny niezależny organ (1.1.1, 1.3.2). Specjalny Sprawozdawca ONZ ds. wolności słowa w raporcie z 2018 r.⁶ wprost rekomenduje, aby państwa powstrzymały się od wprowadzania rozwiązań przewidujących delegowanie odpowiedzialności za ocenę legalności danej treści w internecie na dostawców usług hostingowych, ponieważ mechanizm ten „przedkłada korporacyjny osąd nad wartości wynikające z praw człowieka ze szkodą dla użytkowników” (par. 68). Podobną zasadę zawarto w „Manila Principles of Internet Intermediary Liability”⁷, dokumencie poświęconym roli i odpowiedzialności tzw. pośredników internetowych przygotowanym przez przedstawicieli społeczeństwa obywatelskiego działających na rzecz ochrony praw cyfrowych („Pośrednicy nie mogą być zobowiązani do merytorycznej oceny legalności treści dodawanych przez użytkowników”, IIIa).

W związku z powyższym postulujemy rezygnację z „trybu niewiążącego” i wprowadzenie jednolitego obligatoryjnego trybu usuwania bądź blokowania treści o charakterze terrorystycznym przez dostawców usług internetowych na żądanie uprawnionego organu. Procedura ta wymaga naturalnie obwarowania odpowiednimi gwarancjami (zob. niżej), kluczowe jest jednak, aby zaangażowanie organów państwa w blokowanie bądź usuwanie treści w Internecie opierało się na jasnej, odpowiedzialnej i podlegającej skutecznej weryfikacji ocenie danego materiału w oparciu o przepisy powszechnie obowiązującego prawa.

3. Uwagi dotyczące trybu wiążącego (nakaz usunięcia, art. 4)

Z racji na wysokie ryzyko związane z ograniczeniem wolności słowa, zapobieganie rozpowszechnianiu treści o charakterze terrorystycznym powinno się naszym zdaniem domyślnie odbywać z pełnym zaangażowaniem organów państwowych i pod ich pełną kontrolą. Jednocześnie niezbędne jest skonstruowanie skutecznych mechanizmów gwarancyjnych, z których mogliby skorzystać dostawcy treści.

Autorzy projektu dostrzegli konieczność stworzenia skutecznego środka odwoławczego dla osób, których prawa mogą być naruszone w związku ze stosowaniem projektu (por. motyw 8). „Prawo to obejmuje w szczególności możliwość skutecznego zaskarżenia nakazów usunięcia (...) przed sądem”.

Naszym zdaniem – w zakresie trybu podejmowania decyzji o nakazie usunięcia treści – projekt powinien wprowadzać standard analogiczny do standardu przewidzianego w art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Innymi słowy, wiążący nakaz powinien być wydawany przez niezależny sąd. W związku z tym art. 12 projektu powinien nałożyć na państwa członkowskie obowiązek, by właściwe organy, o których mowa w art. 17 pkt 1 lit. a) nie tylko dysponowały niezbędnymi zdolnościami i wystarczającymi zasobami do realizacji rozporządzenia, ale były także organami niezależnymi od władzy wykonawczej.

W związku z postulowanym przez nas usunięciem z projektu trybu zgłoszeniowego, o którym mowa w art. 5, zadaniem podmiotu właściwego do wykrywania i identyfikacji treści o charakterze terrorystycznym powinno być zwracanie się do sądu z wnioskiem o wydanie nakazu usunięcia na podstawie art. 4.

⁶ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 kwietnia 2018, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35.

⁷ <https://www.manilaprinciples.org/>

4. Proaktywne środki (art. 6)

Projekt sankcjonuje stosowanie przez hostingodawców proaktywnych środków w celu ochrony usług przed rozpowszechnianiem treści o charakterze terrorystycznym, a w pewnych sytuacjach przewiduje nawet obowiązek ich wdrożenia na mocy decyzji „organu nadzorującego”.

Stosowanie proaktywnych środków przez dostawców usług hostingowych w celu moderacji treści jest rozwiązaniem głęboko ingerującym w swobodę wypowiedzi, przede wszystkim z uwagi na ryzyko blokowania treści zgodnych z prawem. W kontekście walki treściami o charakterze terrorystycznym, można wskazać na liczne przykłady nieuzasadnionego blokowania materiałów dokumentujących np. zbrodnie wojenne czy naruszenia praw człowieka w Syrii, które najprawdopodobniej zostały omyłkowo zakwalifikowane jako mające związek z terroryzmem⁸.

Na zagrożenia związane z narzucaniem stosowania proaktywnych środków zwracają uwagę m.in. Sprawozdawca ONZ ds. wolności słowa, instytucje Rady Europy czy środowiska pozarządowe. Zgodnie z rekomendacją Specjalnego Sprawozdawcy ONZ ds. wolności słowa, „państwa powinny powstrzymać się od uchwalania prawa nakazującego stosowanie [przez hostingodawców] proaktywnego monitorowania i filtrowania treści, jako rozwiązań niedających się pogodzić ze standardami prawa do prywatności i stwarzających ryzyko cenzury prewencyjnej” (par. 67)⁹. W raporcie Komitetu Ministrów Rady Europy podkreśla się, że państwa nie powinny wprowadzać obowiązku generalnego monitorowania treści przez pośredników internetowych m.in. z uwagi na ich ograniczoną skuteczność w precyzyjnej ocenie charakteru treści z uwzględnieniem jej szerszego kontekstu (1.3.5, 1.3.8)¹⁰. Organizacja Article19 wskazuje natomiast, że o ile blankietowy obowiązek stosowania proaktywnych środków powinien być co do zasady wykluczony, o tyle jego narzucenie jest możliwe w wyjątkowych przypadkach, pod warunkiem jednak, że odbywa się w sposób maksymalnie transparentny dla użytkowników i może być zakwestionowane przez dostawcę usług hostingowych przed sądem¹¹.

W tym miejscu należy podkreślić, że dostrzegamy i z aprobatą przyjmujemy zaproponowane przez projektodawcę rozwiązania minimalizujące ryzyko nadmiernej ingerencji w prawa podstawowe związane ze stosowaniem proaktywnych środków. Należą do nich: nakaz kierowania się zasadą proporcjonalności przez dostawców usług hostingowych przy ich wdrażaniu, obowiązek uwzględniania swobody wypowiedzi, regulacje dotyczące transparentności, zewnętrznego nadzoru nad środkami proaktywnymi oraz ich ewaluacji. Ponadto projekt przewiduje pewne gwarancje dotyczące stosowania proaktywnych środków w kontekście podejmowania decyzji o zablokowaniu bądź usunięciu treści, nakazując, aby decyzje te były „precyzyjne i uzasadnione”, a także podlegały weryfikacji i nadzorowi przez człowieka. Co więcej, projekt obliguje hostingodawców do notyfikowania dostawców treści o blokadzie/usunięciu treści oraz przewiduje wprowadzenie wewnętrznej procedury odwoławczej od takiej decyzji.

Jednak ze względu na istotne wątpliwości z punktu widzenia proporcjonalności ingerencji w prawa podstawowe, w naszej ocenie przewidziane gwarancje powinny zostać uzupełnione o dwa kluczowe elementy. Po pierwsze, mechanizm skargowy dostępny dla dostawców

⁸ M. Browne, „YouTube Removes Videos Showing Atrocities in Syria”, New York Times, 22 sierpnia 2017, <https://www.nytimes.com/2017/08/22/world/middleeast/syria-youtube-videos-isis.html>

⁹ op. cit.

¹⁰ op. cit.

¹¹ Article 19, How blocking and filtering affect free speech, 2016,

https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf

zablokowanej/usuniętej treści w wyniku stosowania środków proaktywnych (i każdej decyzji podejmowanej w oparciu o wewnętrzne regulacje) nie powinien ograniczać się do wewnętrznej procedury odwoławczej, ale obejmować także możliwość odwołania się od ostatecznej decyzji dostawców usług hostingowych do sądu. Na wymóg poddania takich decyzji kontroli sądowej wprost zwraca uwagę m.in. Komitet Ministrów Rady Europy¹² i OBWE¹³, a także przedstawiciele społeczeństwa obywatelskiego w dokumencie „Santa Clara Principles”¹⁴. Po drugie, uważamy, że rozporządzenie powinno przewidywać możliwość zaskarżenia przez hostingodawcę decyzji organu nadzorującego o nałożeniu obowiązku stosowania proaktywnych środków przed sądem (tymczasem aktualnie w projekcie jest mowa jedynie o możliwości zwrócenia się z wnioskiem o przegląd bądź cofnięcie takiej decyzji do organu, który tę decyzję wydał).

Na marginesie zwracamy uwagę, że zaproponowana regulacja stanowi wyłom (kolejny obok projektu dyrektywy o prawie autorskim na Jednolitym Rynku Cyfrowym) od zasady obowiązującej na gruncie art. 15 unijnej dyrektywy 2000/31/WE o handlu elektronicznym (brak ogólnego obowiązku hostingodawców nadzorowania treści dodawanych przez użytkowników oraz aktywnego badania faktów i okoliczności wskazujących na ich bezprawną działalność).

IV. Przejrzystość i monitorowanie

Popieramy nakładane na hostingodawców obowiązki w zakresie przejrzystości (art. 8). W związku z przedstawionymi wcześniej uwagami dotyczącymi procedury zgłoszeń na podstawie art. 5 projektu, postulujemy (o ile tryb ten zostanie utrzymany), by przedstawiane przez hostingodawców sprawozdania obejmowały zarówno liczbę skierowanych do nich zgłoszeń, jak i liczbę treści, do których dostęp uniemożliwiono.

Zgodnie z art. 21 projektu, państwa członkowskie gromadzą od swoich właściwych organów i dostawców usług hostingowych informacje na temat działań, które podjęli zgodnie z rozporządzeniem, a następnie przesyłają je corocznie Komisji.

W naszej ocenie transparentność procedury uniemożliwiania dostępu do treści jest jednym z kluczowych czynników zmniejszających związane z nią zagrożenia dla wolności słowa. W związku z tym postulujemy wprowadzenie do projektu jednoznacznego rozstrzygnięcia, że informacje przekazywane do Komisji mają charakter jawny i publikowane są na stronach internetowych instytucji odpowiedzialnej za przygotowanie informacji dla Komisji.

V. Podsumowanie

Podsumowując, chcemy podkreślić, że naszym zdaniem dwa największe problemy wynikające z obecnego brzmienia projektu to:

- **nieprecyzyjna definicja treści o charakterze terrorystycznym;**

Pozostawienie jej w obecnym kształcie stwarza realne zagrożenie usuwania treści, których dostępność nie stwarza realnego (lub zgoła żadnego) zagrożenia.

¹² Rekomendacja Komitetu Ministrów Rady Europy w sprawie wolności w Internecie, op. cit.

¹³ OBWE, *A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States*, 2012, s. 52, tekst dostępny na stronie: <http://www.osce.org/fom/105522?download=true> (dostęp: 8.12.2016).

¹⁴ http://globalnetpolicy.org/wp-content/uploads/2018/05/Santa-Clara-Principles_t.pdf

- **dopuszczenie możliwości przeciwdziałania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym w formie nieformalnego zgłoszenia;**

Aktualna propozycja pozostawia swobodę właściwym krajowym organom w wyborze ścieżki działania. Należy przypuszczać, że wybierana będzie ta „wygodniejsza”, to jest zgłoszenia. Tryb ten nie zawiera jednak wystarczających gwarancji dla dostawców treści, a jednocześnie stanowi rezygnację organów państwa na rzecz prywatnych podmiotów z realizacji zadań w zakresie przeciwdziałania terroryzmowi.