Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dn. 16.04.2018 r.
KIGEiT/686/04/2018

Sz. P. Marek Zagórski
Sekretarz Stanu
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Dot. konsultacji Zaleceń Komisji Europejskiej dotyczących walki z bezprawnymi treściami w Internecie.

Szanowny Panie Ministrze.

Działając w imieniu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji (dalej „***Izba***" lub „***KIGEiT***"), odnosząc się do opublikowanego przez Komisję Europejską Zalecenia (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w Internecie, które poprzedza podjęcie przez Komisję działań legislacyjnych w tym zakresie, Izba przedstawia poniższe odpowiedzi na pytania ze strony Ministerstwa Cyfryzacji.

1. *W jaki sposób działania podejmowane przez dostawców usług hostingowych w zakresie skutecznego zwalczania nielegalnych treści w Internecie, powinny wpływać na wyłączenie ich odpowiedzialności (art. 14 Dyrektywy 2000/31/WE)?*

Na wstępie należy zaznaczyć, iż w polskim prawie, na gruncie *uśude*, nie zostały prawidłowo zaimplementowane przepisy art.12-15 Dyrektywy 2000/31/WE (dalej Dyrektywa), co stanowi niezgodność z prawem unijnym i ma bezpośrednio negatywny wpływ na możliwości walki z nielegalnymi treściami w Internecie z uwagi na zbyt szeroko stosowany zakres wyłączeń odpowiedzialności dostawców świadczących usługi hostingowe na terenie Polski.

- W *uśude* zostały nieprawidłowo określone okoliczności zwalniające z odpowiedzialności podmiot świadczący usługę hostingu (niewłaściwa implementacja **art. 14 ust. 1** Dyrektywy, który wskazuje na wyłączenie odpowiedzialności gdy a) *usługodawca nie ma wiarygodnych wiadomości o bezprawnym charakterze działalności lub informacji, a w odniesieniu do roszczeń odszkodowawczych — nie wie o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o tej bezprawności* lub *b) usługodawca podejmuje niezwłocznie odpowiednie działania w*

celu usunięcia lub uniemożliwienia dostępu do informacji, gdy uzyska takie wiadomości lub zostanie o nich powiadomiony"). *Uśude* nie zawiera wyraźnego odwołania się do zawartej w Dyrektywie w odniesieniu do roszczeń odszkodowawczych przesłanki „oczywistości" – tym samym posiadanie przez usługodawcę wiedzy o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o bezprawności informacji lub działalności, nie stanowi na mocy polskich przepisów przesłanki do objęcia usługodawcy odpowiedzialnością, co jest niezgodne z Dyrektywą. Przekładając to na konkretny przykład, w krajach w których Dyrektywa została prawidłowo zaimplementowana dostawca usługi hostingu wie, iż jeżeli określony podmiot regularnie czerpie korzyści z umieszczania przez osoby treści nielegalnych (w tym pirackich), można pociągnąć go do odpowiedzialności.

- Kolejna nieprawidłowość implementacji dotyczy art. 15 ust. 1 Dyrektywy, który zwalnia dostawców jedynie z ogólnego obowiązku monitorowania. Tym samym na mocy Dyrektywy dopuszczone jest wprowadzanie szczególnych obowiązków monitorowania informacji, co znajduje potwierdzenie w orzecznictwie TSUE. Tymczasem *uśude* przewiduje zwolnienie dostawców z jakiegokolwiek obowiązku monitorowania informacji (art. 15 *uśude „Podmiot, który świadczy usługi określone w art. 12–14, nie jest obowiązany do sprawdzania przekazywanych, przechowywanych lub udostępnianych przez niego danych, o których mowa w art. 12–14"*)
- Ponadto w polskim prawie nie zostały w ogóle wdrożone **art. 12 ust. 3, 13 ust. 2 i 14 ust. 3** Dyrektywy, zgodnie z którymi *„wyłączenie usługodawcy od odpowiedzialności nie ma wpływu na możliwość wymagania od usługodawcy przez sąd, żeby przerwał on naruszenia prawa lub im zapobiegł w przyszłości"*. Tym samym w Polsce brak jest przepisów umożliwiających poszkodowanym posiłkowania się wobec hostingodawców, na mocy wyroków sądowych, roszczeniami zakazowymi i/ lub roszczeniami o zapobieżeniu naruszeniom. Wskazane w Dyrektywie wyłączenia od odpowiedzialności nie dotyczą bowiem możliwości nakładania przez sąd na hostingodawców nakazów lub zakazów podjęcia/zaniechania określonych działań.

Dostawcy usług hostingowych celem skorzystania z wyłączeń odpowiedzialności przewidzianych w Dyrektywie powinni co do zasady:

- działać w pełni zgodnie z przepisami Dyrektywy, na bazie przepisów krajowych będących prawidłową i kompletną transpozycją Dyrektywy
- obowiązkowo transparentnie wdrożyć i skutecznie stosować procedurę *notice and take down*, w tym działać niezwłocznie w celu wycofania nielegalnych treści lub uniemożliwienia dostępu do nich)
- optymalnie - obowiązkowo współpracować z sygnalistami (*trusted flaggers*) na jasno określonych i uzgodnionych warunkach (vide także odpowiedź na pytanie nr 2), dostosowanych do specyfiki danej kategorii treści nielegalnych. Dzięki wprowadzeniu przyśpieszonego trybu procedowania zgłoszeń otrzymanych od zaufanych sygnalistów nielegalne treści zostaną szybciej usunięte, a hostingodawca będzie miał większą pewność, iż dane zgłoszenie jest uprawnione i nie narusza praw

podstawowych osoby/podmiotu, który treści te umieścił. Jest to więc rozwiązanie pożądane i zdecydowania korzystne dla podmiotów działających w sposób uczciwy.

Ponadto, można byłoby rozważyć opcjonalne wprowadzenie przez dostawców możliwości samodzielnego blokowania przez uprawnione podmioty treści w Internecie – być może za pomocą wprowadzenia dodatkowego systemu, polegającego na wcześniejszej weryfikacji i stworzeniu konta dla podmiotu uprawnionego/zaufanego sygnalisty (np. w przypadku naruszeń praw własności intelektualnej takimi uprawnionymi byliby nadawcy i organizacje zbiorowego zarządzania prawami autorskimi).

Dostawcy usług hostingowych działający zgodnie z prawem powinni być chronieni przed odpowiedzialnością, w przypadku, gdy dobrowolnie i systematycznie podejmują proaktywne środki w celu identyfikacji szkodliwych treści. Konieczne jest rozwianie wszelkich wątpliwości co do tego, że dostawcy usług hostingowych nie stają się odpowiedzialni za hostowane przez siebie treści, tylko dlatego, że w dobrej wierze podejmują dobrowolne działania, zarówno w sposób zautomatyzowany jak i niezautomatyzowany, zmierzające do identyfikacji i usuwania treści nielegalnych. Powinno być również jasne, że podejmowanie takich działań nie oznacza, że usługodawca ma wiedzę lub kontrolę nad informacjami, które przekazuje lub przechowuje. Dotychczasowy nacisk na zachowanie bierności wobec treści i związana z takim podejściem linia orzecznicza w niektórych Państwach Członkowskich, zniechęcały usługodawców do podejmowania działań zmierzających do usuwania treści bezprawnych.

Z pewnością skuteczności walki z nielegalnymi treściami w Internecie, możliwości jej monitorowania oraz transparentności sprzyjałby obowiązek publikowania sprawozdania z działalności dotyczącej usuwania treści uznawanych za nielegalne oraz uniemożliwiania dostępu do nich. Ponieważ skala obecności nielegalnych treści w Internecie jest duża i staje się narastającym problemem społecznym, a korzystanie z usług hostingodawców jest zjawiskiem powszechnym, w ocenie członków Izby ustanowienie obowiązków sprawozdawczych w tym zakresie jest uzasadnione i proporcjonalne, także biorąc pod uwagę istnienie obowiązków sprawozdawczych w odniesieniu do innych usług, które organy unijne i/lub krajowe uważają za szczególnie istotne ze społecznego punktu widzenia (np. usługi telekomunikacyjne, audiowizualne, finansowe).

Uzgodnione zasady, które będą miały wpływ na wyłączenie odpowiedzialności dostawców usług hostingowych nie powinny być ujęte jedynie w formie zaleceń samoregulacyjnych, lecz mieć odpowiednie przełożenie w przepisach prawa krajowego (np. niezbędne zmiany w *uśude* w tym także umieszczenie zapisów o obowiązku współpracy z sygnalistami; implementacja do prawa krajowego art. 8.3 dyrektywy 2001/29/WE). Wynika to z tego, iż z jednej strony hostingodawcy potrzebują mieć pewność prawną co do skutków podejmowanych przez nich działań lub też zaniechań, a z drugiej z faktu, iż w środowisku internetowym funkcjonuje niemała grupa nieuczciwych podmiotów, które bezpośrednio lub pośrednio czerpią zyski ekonomiczne z udostępniania nielegalnych treści lub świadomie przyczyniają się do propagowania niezgodnych z prawem treści i idei. Podmioty takie z pewnością nie poddadzą się dobrowolnie samoregulacji, gdyż byłoby to sprzeczne z ich interesami.

2. *W jaki sposób należy określić przez dostawców usług hostingowych warunki i kryteria uznania zaufanych podmiotów tzw. „trusted flaggers", aby osiągnąć pluralizm podmiotów?*

O przyznaniu statusu sygnalisty nie powinien decydować jedynie dostawca usług, lecz listy sygnalistów powinny być tworzone we współpracy z różnymi interesariuszami, w tym regulatorami, z uwzględnieniem specyfiki i kategorii treści nielegalnych (np. inna będzie lista sygnalistów w przypadku treści zw. z pornografią dziecięcą i inna w przypadku treści naruszających prawa własności intelektualnej). Zasady przyznawania i funkcjonowania statusu sygnalisty dla danej kategorii treści nielegalnych, jak również zakres danych jakie sygnalista powinien przekazywać, powinny być wypracowane w ramach szerokich konsultacji z udziałem przedstawicieli organów państwowych (np. właściwe ministerstwa, regulatorzy, służby specjalne) przedstawicieli organizacji społecznych, Rzecznika Praw Obywatelskich (RPO), Rzecznika Praw Dziecka (RPD), przedstawicieli biznesu (w tym organizacji i stowarzyszeń branżowych) i właścicieli praw autorskich/OZZ. Niezależnie od ustalenia i opublikowania pierwotnej listy sygnalistów dla danej kategorii treści nielegalnych, (której honorowanie powinno być obowiązkowe dla wszystkich hostingodawców) wraz z jasno określonymi zasadami współpracy dostawców usług hostingowych z tymi sygnalistami, powinien zostać uzgodniony mechanizm cyklicznej weryfikacji statusu sygnalisty oraz procedura nadawania statusu sygnalisty nowym podmiotom w razie potrzeby. W przypadku weryfikacji negatywnej na podstawie jasno określonych przesłanek dostosowanych do kategorii treści nielegalnych, dany podmiot mógłby być usuwany z listy sygnalistów. Weryfikacji co do statusu sygnalisty nie podlegałyby organy państwowe, funkcje typu RPO, RPD.

3. *Czy w sytuacji występowania nielegalnych treści w Internecie jest możliwa skuteczna ochrona, jeśli mamy do czynienia z anonimowym zawiadomieniem i na jakim etapie powinno być ono zgłaszane? W jaki sposób zapobiegać nadużywaniu składania zawiadomień?*

Rozumiemy, iż intencją KE w zapisach rozdziału II art. 7 Komunikatu KE: *„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."* było zapewnienie zawiadamiającym ochrony.

Jednocześnie, pragniemy zwrócić uwagę, iż anonimowość sprzyjać będzie błędnym zgłoszeniom lub nadużyciom. Możliwym rozwiązaniem tego dylematu mogłoby być uzależnienie możliwości zachowania anonimowości od rodzaju zgłaszanych treści nielegalnych.

I tak np. zgłaszający obecność treści terrorystycznych lub zagrażających bezpieczeństwu publicznemu powinien mieć gwarancję anonimowości z uwagi na możliwe zagrożenie/reperkusje wynikające z ew. ujawnienia (nawet niezamierzonego) jego tożsamości.

Z kolei do ustalenia wiarygodności zgłoszenia czy też legalności treści w przypadku praw podmiotowych, takich jak np. prawa własności intelektualnej czy przemysłowej, niezbędne jest ustalenie tożsamości zgłaszającego i otrzymanie jego danych do kontaktu zwrotnego celem przekazania informacji na temat rozstrzygnięcia zgłoszenia. W przypadku naruszeń praw własności intelektualnej i przemysłowej obowiązek podania danych zgłaszającego przyczyniłby się do znacznej eliminacji niezasadnych zgłoszeń lub notyfikacji wynikających z zamierzonych działań anty konkurencyjnych.

Należy również zauważyć, że obowiązek podania danych kontaktowych jest standardową praktyką w wielu procedurach składania wniosków stosowanych na całym świecie. Identyfikacja autora informacji ma krytyczne znaczenie dla mechanizmów dochodzenia roszczeń i przeciwdziałania nadużyciom. Hostingodawcy powinni być także zachęcani do stosowania mechanizmów angażujących użytkowników w zgłaszanie treści potencjalnie bezprawnych (*flagging*). W takich wypadkach, należy dopuścić zgłoszenia anonimowe, w odniesieniu do których zgłaszający nie otrzymuje informacji zwrotnej. Wymóg prowadzenia korespondencji w każdym wypadku takiego zgłoszenia będzie zbyt obciążający dla usługodawców. Równolegle, usługodawcy powinni zapewnić możliwość dokonania zgłoszenia (w ramach procedury *notice and take down*), co do którego zgłaszający zobowiązany jest podać swoją tożsamość i otrzyma informację na temat rozstrzygnięcia zgłoszenia

4. *Jak powinien funkcjonować wzorcowy model pozasądowego rozstrzyganie sporów?*

W ocenie członków Izby nie ma potrzeby wprowadzania dodatkowych regulacji. Zawarcie ugody pozasądowej jest wystarczające.

5. *Jakie zalecenia KE (poza wskazanymi w w/w zaleceniu) powinny być podejmowane przez dostawców usług hostingowych do skutecznego zwalczania nielegalnych treści w Internecie?*

Biorąc pod uwagę negatywne doświadczenia związane z piractwem internetowym, w szczególności zjawisko bardzo szybkiego ponownego pojawiania się nielegalnych treści (np. pod innym linkiem/adresem IP lub nieco zmienioną nazwą) w serwisie hostingodawcy, które zostały już wcześniej przez tego hostingodawcę usunięte, należy dążyć do wprowadzenia mechanizmów procedury „*notice and stay down*" dla treści naruszających prawa własności intelektualnej. W przeciwnym razie walka z piractwem internetowym nigdy nie będzie skuteczna.

W odniesieniu do walki z treściami naruszającymi prawa autorskie w Internecie warto byłoby wzorować się na obowiązującym w USA *Digital Millenium Copyright Act*.

W przypadku zgłoszeń nie anonimowych, dostawcy usług hostingowych powinni przesyłać podmiotowi zgłaszającemu potwierdzenie otrzymania zgłoszenia, proces ten może być oczywiście zautomatyzowany.

6. *Jaka jest najbardziej dogodna formuła zbierania przez właściwy organ sprawozdań dot. zgłoszeń i decyzji dostawców usług hostingowych ws. nielegalnych treści w Internecie?*

Z powyższego pytania nie wynika, czy przyjęta formuła zbierania ma być najbardziej dogodna dla organu, czy też dla podmiotów składających sprawozdanie. Zakładając scenariusz optymalny dla obydwu stron, sprawozdanie powinno być składane nie częściej niż raz w roku, z opcją przekazania w formie elektronicznej (w tym online), na bazie uzgodnionego w ramach konsultacji społecznych szablonu uwzględniającego specyfikę i możliwości dużych oraz małych usługodawców (dla tych drugich byłaby wersja uproszczona). Stworzenie jednolitego stałego szablonu umożliwiłoby jednorazowe przygotowanie systemów raportowych usługodawców do określonych wymogów cyklicznej sprawozdawczości.

Z poważaniem

Prezes Zarządu

Stefan Kamiński