Warszawa, dnia 10 listopada 2022 r.

Sz. P. Janusz Cieszyński
Sekretarz Stanu
Kancelaria Prezesa Rady Ministrów

STANOWISKO
ZWIĄZKU PRACODAWCÓW BRANŻY INTERNETOWEJ INTERACTIVE ADVERTISING BUREAU W/S PROJEKTU USTAWY O OCHRONIE MAŁOLETNICH PRZED DOSTĘPEM DO TREŚCI NIEODPOWIEDNICH W INTERNECIE Z DNIA 6 PAŹDZIERNIKA 2022 R. (UD451)

Szanowni Państwo,

W odpowiedzi na zaproszenie do zgłoszenia uwag do projektu nowej ustawy o ochronie małoletnich przed dostępem do treści nieodpowiednich w internecie (UD451; dalej jako „Projekt"), Związek Pracodawców Branży Internetowej IAB Polska (dalej jako: „IAB Polska") pragnie przedstawić swoje stanowisko.

Członkowie IAB Polska widzą i rozumieją potrzebę zaadresowania rozwiązania dla tak istotnego problemu, jakim jest łatwy i powszechny dostęp małoletnich do treści pornograficznych, które mają szkodliwy wpływ na psychikę młodych ludzi i ich zachowania w relacjach społecznych. Niestety rozwiązania zaproponowane w Projekcie budzą nasze poważne zastrzeżenia i w naszej ocenie wymagają przemodelowania. Główne uwagi przestawiono poniżej.

1. **Błędne główne założenia Projektu w zakresie odpowiedzialności za ochronę małoletnich przed treściami pornograficznymi w sieci.**

Pierwsze zastrzeżenie budzi przyjęte w całej konstrukcji projektu błędne założenie, że to na dostawcach dostępu do internetu spoczywa, pod groźbą wysokich sankcji finansowych, odpowiedzialność za uniemożliwienie małoletnim dostępu do treści pornograficznych w internecie, jak też edukacja społeczeństwa i promocja wiedzy o ochronie dzieci przed szkodliwymi treściami w internecie. Tymczasem obowiązek ochrony małoletnich przed dostępem do pornografii spoczywa przede wszystkich na dostawcach tego typu treści oraz na osobach, które udostępniają je w sieci. Wszak istnieją przepisy polskiego Kodeksu karnego (art. 200), które wyraźnie wskazują:

§ 3. Kto małoletniemu poniżej lat 15 prezentuje treści pornograficzne lub udostępnia mu przedmioty mające taki charakter albo rozpowszechnia treści pornograficzne w sposób umożliwiający takiemu małoletniemu zapoznanie się z nimi, podlega karze pozbawienia wolności do lat 3.
§ 4. Karze określonej w § 3 podlega, kto w celu swojego zaspokojenia seksualnego lub zaspokojenia seksualnego innej osoby prezentuje małoletniemu poniżej lat 15 wykonanie czynności seksualnej.
§ 5. Karze określonej w § 3 podlega, kto prowadzi reklamę lub promocję działalności polegającej na rozpowszechnianiu treści pornograficznych w sposób umożliwiający zapoznanie się z nimi małoletniemu poniżej lat 15.

Z powyższych przepisów wynika, iż to właśnie osoby prezentujące treści/dostawcy treści pornograficznych są odpowiedzialni za uniemożliwienie dostępu do takich treści małoletnim. Dlatego projekt ustawy powinien przede wszystkim być adresowany do osób i podmiotów prezentujących pornografię w internecie i nałożyć na nie obowiązek wdrożenia skutecznych mechanizmów weryfikacji wieku (na pewno nie jest nim kliknięcie przez użytkownika w okienko „Mam skończone 18 lat"). Nie jest to skomplikowane, wszak skuteczne zabezpieczenia techniczne są już stosowane od wielu lat przez legalnie działających dostawców VoD. Ponadto, projekt ustawy powinien zawierać surowe przepisy odnoszące się do egzekucji tego obowiązku. Jest niezrozumiałym, dlaczego polski ustawodawca nie chciał zaczerpnąć z przykładu takich krajów jak Niemcy i Francja, które oprócz powyżej wspomnianego obowiązku identyfikacji wieku przez podmioty prezentujące treści pornograficzne wprowadziły blokowanie przez dostawców dostępu do internetu stron podmiotów naruszających przepisy o weryfikacji wieku. Blokada taka jest zakładana na wniosek sądu lub właściwego organu.

Warto zauważyć, że w Polsce od lat funkcjonuje już mechanizm blokowania domen internetowych (na podstawie rejestru wprowadzonego na mocy przepisów ustawy o grach hazardowych). Tym samym na gruncie polskim istnieją rozwiązania techniczne i prawne, które przy stosunkowo prostej modyfikacji mogłyby w sposób właściwy i sprawiedliwy zminimalizować problem dostępu małoletnich do pornografii w sieci.

Należy także wyraźnie wskazać, że to przede wszystkim na rodzicach oraz na organach państwa spoczywa obowiązek edukacji dzieci w zakresie bezpiecznego korzystania z internetu. Jest to konieczny element całego procesu wychowawczego i kluczową rolę powinni tu odgrywać rodzice, szkoły oraz właśnie państwo, poprzez odpowiednie programy szkoleniowe adresowane do dzieci i rodziców, kampanie promocyjne i informacyjne. Należy przede wszystkim w pełni wykorzystać istniejące rozwiązania, w które zainwestowano już środki publiczne, np. stworzoną przez NASK aplikację mOchrona[1] - dostępne publicznie i bezpłatne narzędzie ochrony rodzicielskiej. Powstaje pytanie, dlaczego rodzice nie instalują masowo takiego istniejącego już darmowego narzędzia na telefonach swoich dzieci? Prawdopodobnie zabrakło odpowiedniej

[1] https://www.nask.pl/pl/aktualnosci/4365,Aplikacja-mOchrona-stworzona-dla-rodzicow-z-mysla-o-dzieciach.html

promocji i edukacji. Przedsiębiorcy telekomunikacyjni nie mogą być zobowiązywani pod groźbą sankcji finansowych do wyręczania państwa w zakresie edukowania społeczeństwa i promowania właściwych zachowań.

Aktywne włączenie się państwa w stworzenie przemyślanej strategii komunikacyjnej w zakresie ochrony małoletnich przed niebezpiecznymi treściami w internecie (nie tylko pornografią) jest o tyle istotne, że nie istnieje rozwiązanie techniczne gwarantujące 100% skuteczności blokowania; każde rozwiązanie można obejść (a młodzi ludzie mają sporą wiedzę techniczną i potrafią znaleźć w sieci instrukcje jak poradzić sobie z niechcianą blokadą); dodatkowo dostawcy internetu nie mają możliwości blokowania treści pornograficznych pochodzących z ruchu szyfrowanego.

Warto także byłoby jeszcze bardziej włączyć NASK w proces ochrony małoletnich przez treściami pornograficznymi, np. powierzając tej doświadczonej w zakresie szeroko pojętego bezpieczeństwa w internecie instytucji prowadzenie scentralizowanego rejestru domen naruszających przepisy prawa w zakresie prezentowania treści pornograficznych. Na podstawie takiego rejestru operatorzy telekomunikacyjni mogliby zakładać blokady. Byłoby to rozwiązanie o tyle skuteczne, że:

- zablokowanie domeny skutkowałoby brakiem dostępu dla wszystkich, także pełnoletnich użytkowników, co szybko odcięłoby właściciela domeny od monetyzacji (opłata za treści, przychody z reklam) i skłoniło go do wdrożenia odpowiednich zabezpieczeń weryfikujących wiek;
- zapewniłoby blokowanie takiego samego zbioru nielegalnych domen przez wszystkich operatorów w Polsce;
- umożliwiłoby skuteczne i jednolite egzekwowanie polskich przepisów wobec naruszających prawo podmiotów działających za granicą i kierujących treści pornograficzne do odbiorców w Polsce.
- poprzez przyjęcie jednolitego podejścia do sposoby kwalifikacji treści jako pornografii, w mniejszym stopniu naruszałoby zasadę otwartego internetu, gdyż pozwoliłoby uniknąć mozaiki filtrów i algorytmów stosowanych w różnym zakresie i skali przez poszczególnych dostawców internetu.

2. **Brak definicji treści pornograficznych – przerzucenie na dostawców internetu obowiązku weryfikowania co stanowi taką treść, przy jednoczesnych wysokich karach finansowych w przypadku, gdy organ kontrolny nie zgodzi się ze sposobem kwalifikacji danych treści.**

Kwestia ta rodzi poważne obawy członków IAB Polska. W Uzasadnieniu do Projektu wskazano, że ustawa celowo nie definiuje treści pornograficznych, lecz pozostawia pole do interpretacji dostawcom internetu. Jednocześnie w tymże Uzasadnieniu przytaczane są zróżnicowane definicje takich treści. Trudno zgodzić się z argumentacją, że zdefiniowanie pornografii zależy od aspektów kulturowych, skoro poruszamy się w obrębie polskiej kultury i prawa polskiego, a

nie np. unijnego. Ponadto, nietrafione są argumenty z Uzasadnienia odnoszące się do zmian technologicznych w zakresie przechowywania treści w internecie, czy sposobu ich produkcji, jako czynników uniemożliwiających zdefiniowanie pornografii, gdyż że w praktyce nie odgrywają one roli podczas oceny co jest, a co nie jest pornografią. Zdaniem członków IAB Polska projektodawca uchyla się od odpowiedzialności za wskazanie optymalnej definicji pornografii przy jednoczesnym nakazie blokowania niezdefiniowanych treści i nałożeniu surowych kar finansowych za niewłaściwe w ocenie organu kontrolującego blokowanie. Taki sposób stanowienia prawa budzi nasz stanowczy sprzeciw, jako że jest nieracjonalny, niesprawiedliwy i stanowi całkowite ignorowanie zasady pewności prawa.

Należy pamiętać, że dostawcy ISP są przedsiębiorcami telekomunikacyjnymi, a nie podmiotami biegłymi w dziedzinie pornografii czy psychologii dziecięcej i nie może być im przypisywana kompetencja należąca do wyspecjalizowanego organu/instytucji lub sądu. Ocena tego co jest, a co nie jest pornografią jest trudna i często subiektywna. Zwracamy również uwagę, za *https://opornografii.pl*, że:

> *(…) termin "treści pornograficzne" jest według orzecznictwa pojęciem prawnym, a nie pojęciem medycznym, czy seksuologicznym. W wyroku z dnia 23 listopada 2010 r. (IV KK173/10) Sąd Najwyższy wyraźnie stwierdza, że ocena, czy dana treść ma charakter pornograficzny, należy do sądu, a nie do biegłego. Biegły może co najwyżej ocenić, jaki hipotetyczny wpływ na konkretną osobę ma prezentowana treść. Scedowanie kwalifikacji danej treści na biegłego zostało jednoznacznie skrytykowane przez Sąd Najwyższy. Jak podkreśla Sąd Okręgowy w Warszawie (wyrok niepublikowany: Sygn. akt. XX GC 1052/14), na gruncie ustawy o radiofonii i telewizji: "definicji [treści pornograficznych] faktycznie wskazać można wiele, konstruowanych wedle różnych metod i kryteriów, zawsze jednak pamiętać należy o ich raczej projektującym niźli regulującym charakterze i istniejącym marginesie wątpliwości co do desygnatów, wyznaczonych treścią tych definicji w przypadkach trudnych, granicznych i wyjątkowych. Zawsze więc ostateczna decyzja co do identyfikacji i wskazania desygnatów tych pojęć należeć będzie do podmiotu oceniającego, w szczególności do sądu"*[2]

3. Problem z wykonaniem obowiązków w stosunku do użytkowników pre-paid

Operatorzy nie widzą możliwości proponowania użytkownikowi prepaid włączenia blokady przed zawarciem umowy w przypadku, gdy karta SIM nabywania jest poza punktem sprzedaży prowadzonym przez operatora (np. w marketach, na stacjach benzynowych).

4. Obawy dotyczące naruszenia prywatności użytkowników

[2] https://opornografii.pl/article/czy-i-jak-definiowac-pornografie-na-potrzeby-postepowan-sadowych

Identyfikacja ruchu sieciowego zawierającego treści pornograficznej wymaga w praktyce stosowania technologii Deep Packet Inspection, która mocno ingeruje w prywatność wszystkich użytkowników, jako że wiąże się z monitorowaniem całego nieszyfrowanego ruchu internetowego. Można spodziewać się, iż praktyka taka wzbudzi sprzeciw wielu Polaków i organizacji pozarządowych, gdyż w niektórych krajach bywa wykorzystywana do inwigilacji i tak jest powszechnie kojarzona. Niezależnie, konieczność wykazania przez dostawcę dostępu do internetu przestrzegania obowiązków wiąże się ze zbieraniem danych użytkowników, co dla osób które rezygnują z blokady może być problematyczne, gdyż są to informacje na pograniczu danych wrażliwych i w przypadku wyrywkowej kontroli operatora użytkownik może nie życzyć sobie, aby organ kontrolujący miał dostęp do tego typu informacji o nim.

5. Niezgodność projektowanych przepisów z prawem unijnym

Podkreślenia wymaga fakt, że ochrona małoletnich przed dostępem do treści nieodpowiednich powinna odbywać się jedynie w sposób zgodny z przepisami obowiązującego prawa (krajowego oraz unijnego), a także z uwzględnieniem zasady neutralności sieci (w myśl której podmiot dokonujący transmisji nie ma wpływu na to jaka treść jest transmitowana) oraz instrumentów samoregulacji oraz współregulacji branżowej.

Należy zauważyć, że w prawodawstwie Unii Europejskiej dotyczącym tzw. sektora komunikacji elektronicznej, a w konsekwencji również w krajowym porządku prawnym wyraźnie oddziela się *„regulacje dotyczącą transmisji”* (ang. *regulation of transmission*) od *„regulacji dotyczącej treści rozpowszechnionych w sieci”* (ang. *regulation of content*). Zasadę tą podkreślono jednoznacznie w *„Dyrektywie 2002/21/WE o wspólnych ramach prawnych dla sieci i usług komunikacji elektronicznej*.” Problematyka pornografii zalicza się niewątpliwie do drugiej z w/w grup tj. grupy zagadnień *„contentowych*” (treściowych). Pomimo powyższego Projekt przewiduje regulowanie kwestii dostępu do niej za pośrednictwem *„regulacji dotyczących transmisji”* co jest sprzeczne z w/w zasadą neutralności sieci.

W treści przepisów art. 12 – 14 *Dyrektywy 2000/31/WE w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)* ustanowiono odrębne zasady odpowiedzialności podmiotów pośredniczących w dostępie do treści osób trzecich (ang. INTERMEDIARY SERVICE PROVIDERS - ISP) z tytułu przechowywania lub przekazywania bezprawnych danych lub danych, z którymi jest związana bezprawna działalność.

Powyższe dotyczy trzech kategorii ISP czyli: (1) podmiotów świadczących usługi „zwykłego przekazu” (np. operator telekomunikacyjny, dostawca usługi dostępu do Internetu), (2) „hostingu” (np. podmiot udostępniający serwery na cele prowadzenia strony internetowej) oraz (3) „cachingu” (np. podmiot, którego serwery służą innym podmiotom do transmisji danych).

Natomiast w myśl art. 15 ust.1 Dyrektywy 2000/31/WE państwa Członkowskie UE (w tym również RP) nie nakładają na ISP (a więc również dostawców usług dostępu do Internetu): a)

„ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują" ani b) „ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność".

W konsekwencji ustawodawca polski wprowadził do „Ustawy o świadczeniu usług drogą elektroniczną" przepis art. 15, w myśl którego:

> *Podmiot, który świadczy usługi określone w art. 12-14 (tj. zwykłego przekazu, hostingu oraz cachingu), nie jest obowiązany do sprawdzania przekazywanych, przechowywanych lub udostępnianych przez niego danych, o których mowa w art. 12-14.*

Zgodnie ze zmianami, jakie wprowadzi opublikowane niedawno rozporządzenie: Akt o usługach cyfrowych („AUC")[3] i które będzie stosowane od dnia 17 lutego 2024 r. - wskazane powyżej art. 12-15 Dyrektywy 2000/31/WE zostaną uchylone i zastąpione art. 4, 5, 6 i 8 AUC. Odesłania do art. 12–15 dyrektywy 2000/31/WE odczytuje się jako odesłania odpowiednio do ww. przepisów AUC. Wobec powyższego, art. 8 AUC (za art. 15 Dyrektywy) oraz uzasadniający go motyw 30) rozporządzenia utrzymują zakaz nakładania przez Państwa członkowskie ogólnego obowiązku monitorowania treści przed dostawców usług pośrednich:

> *art. 8 - Na dostawców usług pośrednich* ***nie nakłada się ogólnego obowiązku monitorowania informacji****, które dostawcy ci przekazują lub przechowują, ani aktywnego ustalania faktów lub okoliczności wskazujących na nielegalną działalność.*
>
> *mot. 30) - Na dostawcach usług pośrednich* ***nie powinien spoczywać obowiązek monitorowania – ani na mocy prawa, ani w praktyce – w odniesieniu do obowiązków o charakterze ogólnym****. Nie dotyczy to obowiązków monitorowania w konkretnym przypadku oraz, w szczególności, nie wpływa to na nakazy organów krajowych wydane zgodnie z ustawodawstwem krajowym zgodnym z prawem Unii, stosownie do wykładni Trybunału Sprawiedliwości Unii Europejskiej, oraz zgodnie z warunkami ustanowionymi w niniejszym rozporządzeniu. Żadnego z przepisów niniejszego rozporządzenia nie należy interpretować jako nałożenia ogólnego obowiązku monitorowania ani ogólnego obowiązku aktywnego ustalania faktów, ani też jako nałożenia na dostawców ogólnego obowiązku podejmowania aktywnych działań w odniesieniu do nielegalnych treści.*

Należy zatem uznać, że obecne przepisy UE oraz prawa krajowego nie zezwalają Rządowi RP na nałożenie na dostawców usług dostępu do internetu obowiązku blokowania przesyłania treści o jakimkolwiek charakterze, w tym treści pornograficznych.

---

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych); Dz.U. L 277 z 27.10.2022, str. 1—102.

Warto zauważyć, że podczas dokonywania czynności mających na celu ograniczenie dostępu do treści o charakterze pornograficznym dostawca usług internetowych byłby zobowiązany poddać stałemu nadzorowi wszystkie przekazywane przez siebie dane i w konsekwencji obowiązek taki miałby charakter ogólny.

Tymczasem obecnie obowiązująca dyrektywa 2000/31/WE dopuszczają jedynie możliwość nałożenia obowiązków o charakterze określonym w motywie (47) Preambuły do w/w Dyrektywy czyli obowiązków w tzw. „przypadkach szczególnych", które – zdaniem IAB Polska - należy rozumieć jako zgodne z polskim prawem procesowym nakazy sądu (np. postanowienia o zabezpieczeniu powództwa, w wyniku których pozwany jest zobowiązywany do zablokowania treści na określony czas), które mają charakter: a) jednostkowy (incydentalny), b) ograniczony w czasie (np. na czas trwania procesu) oraz c) odnoszący się do konkretnego stanu faktycznego i precyzyjnie określonych danych (np. konkretnych plików), a nie tylko ich kategorii. Jak bowiem stwierdzono w motywie (47) Preambuły:

> *Państwa Członkowskie nie mogą nakładać na usługodawców obowiązku nadzoru jedynie w odniesieniu do obowiązków o charakterze ogólnym; nie dotyczy to obowiązków nadzoru mających zastosowanie do przypadków szczególnych oraz, w szczególności, nie ma wpływu na decyzje władz krajowych podjęte zgodnie z ustawodawstwem krajowym.*

Analogicznie do przywołanego powyżej uzasadnienie znajduje się również w AUC, odpowiednio w motywie 30) i następnych tego rozporządzenia. Wobec czego aktualna pozostaje następująca wykładnia:

„Przyczyną wprowadzenia przez prawodawcę wspólnotowego, a za nim przez ustawodawcę polskiego, powyższej regulacji (art. 15 „Ustawy o świadczeniu usług drogą elektroniczną" – przyp. IAB Polska) jest niezmiernie duża ilość danych, jakie są przekazywane lub przechowywane przez usługodawców wskazanych w art. 12 – 14 u.ś.u.d.e. (M. Świerczyński, w: Ustawa o świadczeniu usług drogą elektroniczną. Komentarz, red. J. Gołaczyński, Warszawa 2009r., str. 135). W związku z tym dopuszczenie możliwości wprowadzenia generalnego obowiązku monitorowania przez usługodawców przekazywanych lub przechowywanych danych prowadziłoby do powstania po ich stronie niemożliwej do spełnienia powinności. Jednocześnie koszty, jakie byłyby konieczne do wprowadzenia programów komputerowych filtrujących dane lub do zatrudnienia wystarczającej liczby pracowników sprawdzających dane pod względem ich bezprawności, byłyby bardzo duże. Mogłyby one postawić pod znakiem zapytania opłacalność działalności podmiotów, o których mowa w art. 12 -14 u.ś.u.d.e. Na marginesie należy zaznaczyć, że tego typu rozwiązania i tak nie byłyby w pełni skuteczne (podkr. – IAB Polska) (zob. G.Spindler, Ch. Volkmann, Die zivilrechtliche Storerhaftung der Internet – Provider, WRP 2003, nr 1, s. 9; G. Spindler w: G. Spindler, P. Schmitz, I. Geis, TDG

Teledien stegesetz, Teledienstedatenschutzgesetz, Signaturgesetz, Kommentar, Munchen 2004, s. 177) z uwagi na możliwość łatwego obejścia programów filtrujących[4].

Mając na uwadze wszystkie przytoczone powyżej argumenty nie należy zgodzić się z zawartym w uzasadnieniu do Projektu (art. 21) stwierdzeniem, że projekt ustawy nie jest objęty zakresem prawa Unii Europejskiej.

6. Termin wejścia w życie projektowanych przepisów

Wyrażamy głęboką nadzieję, że przedstawiona przez nas we wcześniejszej części stanowiska argumentacja zyska zrozumienie ustawodawcy i Projekt zostanie znacznie zmieniony. Gdyby jednak tak się nie stało pragniemy wskazać, że zaproponowany w Projekcie termin trzech miesięcy na wejście obowiązków dla dostawców przekraczających próg 4 mln zł przychodu jest stanowczo zbyt krótki. Projektowane przepisy wymagają szeregu zmian w procesach obsługi klienta, dokumentacji i przede wszystkim w systemach dostawców dostępu do internetu. Dostawcy tacy oferują obecnie płatne i bezpłatne rozwiązania ochrony rodzicielskiej (często w oparciu o umowy z dostawcami zewnętrznymi), nie są one jednak tożsame z rozwiązaniami jakie musieliby wdrożyć na podstawie projektowanej ustawy. Tym samym, dla tejże grupy dostawców, wnioskujemy o wejście w życie przepisów po 12 miesiącach od publikacji.

7. Notyfikacja Komisji Europejskiej

W uzasadnieniu do Projektu stwierdzono, że w Projekcie nie zawarto przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597; dalej jako: „Rozporządzenie") oraz że nie zachodzi konieczność notyfikacji Komisji Europejskiej. W ocenie IAB Polska takie stwierdzenie nie jest prawidłowe. Rozporządzenie, o którym mowa powyżej jest aktem prawnym implementującym Dyrektywę 2015/1535 z dnia 9 września 2015 r. ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego. Zarówno wspomniane powyżej Rozporządzenie, jak i dyrektywa wymagają notyfikacji Komisji Europejskiej, w przypadku kiedy w projektowanym akcie prawnym znajdują się *przepisy techniczne. Przepisy techniczne* to, zgodnie z wyżej wspomnianą dyrektywą i Rozporządzeniem, także przepisy dotyczące usług (§ 2 pkt 5 lit. c Rozporządzenia). Z kolei usługa, to zgodnie z § 2 pkt 1 usługa *w ramach społeczeństwa informacyjnego, świadczona za wynagrodzeniem, bez równoczesnej obecności stron (na odległość), poprzez przesyłanie danych na indywidualne żądanie usługobiorcy, przesyłana pierwotnie i otrzymywaną w miejscu przeznaczenia za pomocą sprzętu do elektronicznego przesyłania i przechowywania danych, włącznie z kompresją cyfrową, która jest w całości przesyłana, kierowana i otrzymywana za pomocą kabla, drogą radiową, przy użyciu środków optycznych lub innych środków elektromagnetycznych (drogą elektroniczną).* Dostarczanie treści pornograficznych co do

[4] W. Chomiczewski w: „Świadczenie usług drogą elektroniczną oraz dostęp warunków – Komentarz do ustaw" red. Dominik Lubasz i Monika Namysłowska, Wydanie 1, Warszawa,, str. 249/250

zasady stanowi usługę w rozumieniu Rozporządzenia. Wobec czego w ocenie IAB Polska konieczna jest notyfikacja do Komisji Europejskiej, ponieważ przepisy zawarte w Projekcie stanowią *przepisy techniczne* w rozumieniu Rozporządzenia, w zakresie w jakim wpływają one i ograniczają możliwość świadczenia usług społeczeństwa informacyjnego. Celem notyfikacji projektu regulacji do Komisji Europejskiej jest umożliwienie oceny, czy projektowany akt prawny nie narusza przepisów prawa Unii Europejskiej, szczególnie tych które gwarantują swobodny przepływ usług społeczeństwa informacyjnego w ramach rynku wewnętrznego.

Ponadto wskazujemy, że w odniesieniu do Projektu nie zachodzi wyłączenie z § 4 ust. 2 pkt 1 Rozporządzenia, ponieważ Projekt zawiera przepisy tworzące obowiązki, które nie są objęte regulacjami unijnymi oraz zawiera przepisy, które mogą mieć bezpośredni wpływ na swobodę przepływu usług świadczonych drogą elektroniczną na rynku wewnętrznym Unii Europejskiej, a nie wyłącznie dotyczące usług telekomunikacyjnych.

Z poważaniem,

Włodzimierz Schmidt
Prezes Zarządu