

## **Stanowisko Polskiej Izby Informatyki i Telekomunikacji wobec projektu ustawy o ochronie małoletnich przed dostępem do treści nieodpowiednich w internecie (druk sejmowy nr 3282)**

### **WPROWADZENIE I POSTULATY KIERUNKOWE**

Treści i usługi dostępne za pośrednictwem sieci internet (potocznie „w internecie”) są odbiciem społeczeństw, gospodarek, polityki, kultury i technologii całej ludzkości. Internet jest jednym z największych technologicznych wynalazków ludzkości, który przyczynił się i wciąż przyczynia się do bezprecedensowego postępu w zasadzie we wszystkich dziedzinach życia. Korzyści płynące z otwartego internetu można wymieniać bardzo długo, ale te są znane i chyba nikogo nie trzeba przekonywać o tym, jaką wartością i jak ważny jest dostęp do internetu i jakim problemem jest brak tego dostępu. Niestety, tak jak w świecie „realnym”, tak i w świecie wirtualnym są treści, usługi i zachowania nielegalne albo takie, które uważa się za niepożądane lub szkodliwe, w szczególności jeśli odbiorcą tych treści jest dziecko, osoba małoletnia. W świecie „realnym” chronimy dzieci przed zagrożeniami przede wszystkim przez rozmowę, poświęcanie uwagi, wychowywanie, uświadamianie i edukowanie, jak unikać zagrożeń i jak sobie radzić w sytuacji zagrożenia.

Nikt nie ma wątpliwości, że jest to rola i odpowiedzialność rodziców i systemu edukacji. Jeśli w świecie „realnym” stosujemy w tym zakresie jakieś rozwiązania techniczne, to tylko i wyłącznie jako wsparcie i uzupełnienie dla wychowywania, uświadamiania i edukowania dzieci, a nie jako narzędzia zastępujące uwagę, którą jako rodzice jesteście winni dzieciom.

Pamiętać trzeba, że tak jak w świecie realnym, tak w świecie wirtualnym dostępnych jest bardzo wiele rozwiązań technicznych, zarówno odpłatnych, jak i darmowych, które pomagają chronić dzieci, wystarczy wola i wiedza rodziców i opiekunów, aby z tych narzędzi korzystać. Nie ma żadnego powodu, aby zagrożenia w świecie wirtualnym traktować diametralnie odmiennie od zagrożeń w świecie realnym, a fundamenty i zasady ochrony dzieci przed zagrożeniami w obu tych światach powinny być takie same. Rozwiązania techniczne i normy prawne, w szczególności błędnie zaadresowane i skonstruowane, pozbawione podstawy, jaką jest uwaga rodzicielska, wychowywanie i edukowanie mogą wręcz pogłębić problem, gdyż stworzą po stronie rodziców, polityków i w mediach fałszywe wrażenie bezpieczeństwa i „załatwienia sprawy”, podczas gdy dzieci, które – jeśli zechcą – bez większego wysiłku ominą zabezpieczenia techniczne i będą narażone na wszystkie treści i usługi dostępne za pośrednictwem sieci internet. Tym bardziej, jeśli projektowane rozwiązania prawne adresują jedynie niewielki wycinek treści, które mogą być szkodliwe dla dzieci, a więc problem treści pornograficznych. W średniej perspektywie czasowej może pojawić się pokusa, aby bezpieczeństwo dzieci w internecie w całości powierzyć jedynie rozwiązaniom technicznym i dostawcom technologii nie tylko w zakresie treści pornograficznych, ale również innych treści i usług, które mogą być szkodliwe dla dzieci.

Ochrona dzieci przed dostępem do nieodpowiednich treści jest bez wątpienia jednym z większych wyzwań z jakim musimy się zmierzyć jako rodzice, społeczeństwo i Państwo Polskie.

Rząd, przedkładając projektowaną ustawę, bez wątpienia trafnie zidentyfikował problem, jakim jest stosunkowo łatwy dostęp przez małoletnich do treści pornograficznych, niestety zaproponował błędne, nieuzasadnione i zwyczajnie niesprawiedliwe remedium, które całą odpowiedzialność za bezpieczeństwo

dzieci w świecie wirtualnym składa na barki przedsiębiorców telekomunikacyjnych zapewniających dostęp do sieci internet, ograniczając rolę rodzica do wnioskowania o usługę, a rolę Państwa Polskiego do recenzowania wysiłków dostawców internetu. Dostawcy internetu mają nie tylko zapewnić funkcjonowanie usługi blokującej dostęp do treści pornograficznych, ale zgodnie z projektowaną ustawą mają prowadzić działania informacyjne, a więc mają - w reżimie obowiązku realizowanego pod groźbą kary pieniężnej – realizować zadania i funkcje, które w sposób oczywisty są zadaniami Państwa Polskiego i powinny być realizowane w ramach polityki społecznej i rodzinnej (Ministerstwo Rodziny i Polityki Społecznej), systemu edukacji (Ministerstwo Edukacji i Nauki, szkoły i nauczyciele) i z wykorzystaniem licznych, opłacanych z budżetu państwa, instytucji, które mają dbać o dzieci (Rzecznik Praw Dziecka), o bezpieczeństwo komunikacji elektronicznej (Prezes Urzędu Komunikacji Elektronicznej) i realizować misję publiczną w mediach (telewizja i radio publiczne).

Model i rozwiązania zaproponowane w projektowanej ustawie są niewłaściwe zaadresowane, nieuzasadnione i nietrafione z następujących powodów, które zostaną szerzej przedstawione w dalszej części niniejszego stanowiska:

1. naruszają prawo Unii Europejskiej, a projekt ustawy powinien być notyfikowany Komisji Europejskiej (obowiązek notyfikacji nie został wykonany);
2. ignorują obowiązujące już w Polsce przepisy prawa, których celem jest ograniczenie dostępności pornografii dla małoletnich;
3. deprecjonują wagę i rolę wychowania i edukacji;
4. pomijają fakt, że już dzisiaj istnieje cała gama rozwiązań technicznych służących ochronie małoletnich przed nieodpowiednimi treściami, zarówno odpłatnych jak i darmowych (w tym rozwiązań darmowych stworzonych z wykorzystaniem środków publicznych), prostych w obsłudze i dostępnych dla każdego, kto chce z nich korzystać;
5. w sposób nieuzasadniony i zwyczajnie niesprawiedliwy adresują wszystkie obowiązki na dostawców internetu, pozostawiając dostawców treści dla dzieci szkodliwych, w tym dostawców treści pornograficznych, całkowicie poza zakresem zainteresowania Projektodawcy i projektowanej ustawy;
6. nakładają na dostawców internetu obowiązki prowadzenia działań informacyjnych dotyczących blokad i treści pornograficznych, które mają być realizowane pod groźbą kary, a więc przerzucają na prywatne przedsiębiorstwa realizację należących do Państwa Polskiego zadań z zakresu edukacji, polityki rodzinnej i społecznej;
7. tworzą fałszywą wizję możliwości rozwiązania skomplikowanego problemu społecznego przez proste nakazy i zakazy ustawowe, dając złudne poczucie bezpieczeństwa;
8. stwarzają polityczną pokusę do obejmowania obowiązkiem blokowania kolejnych kategorii treści i usług uznawanych za szkodliwe albo niepożądane;
9. stwarzają nowe, poważne ryzyka dla prywatności abonentów;
10. z niezrozumiałych powodów proponują model nieznanym w żadnym innym państwie, odmienny od tego, który został albo jest wdrażany w niektórych państwach Europy.

Wszystkie powyżej zasygnalizowane zastrzeżenia zostały opisane szczegółowo w dalszej części niniejszego stanowiska, a w tym miejscu pragniemy przedstawić nasze postulaty kierunkowe:

1. sugerujemy, aby Państwo Polskie wraz z jego instytucjami (takimi jak Ministerstwo Rodziny i Polityki Społecznej, Ministerstwo Edukacji i Nauki, Rzecznik Praw Dziecka, Prezes Urzędu Komunikacji Elektronicznej, publiczna telewizja i radio) skupiło się na działaniach edukacyjnych i informacyjnych, adresowanych zarówno do rodziców i opiekunów jak i dzieci, których celem będzie zwiększenie świadomości na temat zagrożeń jak również na temat sposobów i dostępnych

już dzisiaj rozwiązań (w tym narzędzi technicznych) pomagających – każdemu chcącemu z nich korzystać – w chronieniu dzieci nie tylko przed dostępem do nieodpowiednich treści (rozumianych znacznie szerzej niż tylko treści pornograficzne), ale również pomagających w kontrolowaniu aktywności dzieci w świecie wirtualnym oraz kształtowaniu prawidłowych wzorców zachowań i postaw wobec uzależnień i innych zagrożeń związanych z elektroniką i światem cyfrowym (kontrola rodzicielska, programy antywirusowe i znacznie więcej);

2. zamiast na tworzeniu nowych regulacji prawnych sugerujemy skupienie uwagi Państwa Polskiego na egzekwowaniu już istniejących regulacji prawnych, których celem jest ochrona małoletnich przed dostępem do treści pornograficznych, takich jak art. 200 § 3 i 5 Kodeksu karnego, które przewidują karę pozbawienia wolności do lat 3 dla każdego, kto:
  - a. 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
  - b. prowadzi reklamę lub promocję działalności polegającej na rozpowszechnianiu treści pornograficznych w sposób umożliwiający zapoznanie się z nimi małoletniemu poniżej lat 15;
3. jeśli w ocenie Projektodawcy przyjęcie nowych regulacji prawnych jest konieczne, to takie rozwiązania powinny być wzorowane na działających rozwiązaniach wdrożonych w innych krajach, np. we Francji, w Niemczech i wdrażanych w Wielkiej Brytanii, które Projektodawca opisuje w Ocenie Skutków Regulacji (OSR) do projektowanej ustawy, a które znacznie lepiej adresują problem i są pozbawione większości najpoważniejszych wad i ryzyk zasygnalizowanych wcześniej; docelowe przepisy powinny:
  - a. wymagać od dostawców treści pornograficznych skutecznej weryfikacji wieku użytkownika celem odmówienia dostępu użytkownikowi niepełnoletniemu (co stanowiłoby naturalne i logiczne uzupełnienie przytoczonego już wcześniej przepisu polskiego Kodeksu karnego);
  - b. przewidywać, że domena internetowa dostawcy treści pornograficznych, który nie wdroży skutecznego mechanizmu weryfikacji wieku albo udziela dostępu osobom niepełnoletnim po weryfikacji wieku, jest wpisywana do rejestru domen internetowych, które byłyby w tym modelu blokowane przez dostawców usługi dostępu do sieci internet.

Dostawcy usługi dostępu do sieci internet mogą być częścią kompleksowej kampanii i systemowych działań zmierzających do ograniczenia ekspozycji małoletnich na treści pornograficzne, ale rola dostawców internetu powinna być adekwatna do roli i funkcji jaką w gospodarce i społeczeństwie pełnią przedsiębiorcy telekomunikacyjni, uwzględniając potrzebę zaadresowania u źródła problemu dostępu przez małoletnich do treści pornograficznych, a więc na poziomie dostawców treści pornograficznych. Taki właśnie model został wdrożony we Francji oraz w Niemczech i jest wdrażany w Wielkiej Brytanii.

W kolejnej części stanowiska prezentujemy uwagi kierunkowe, czyli takie, które w ocenie Izby dyskwalifikują projektowaną ustawę w obecnym kształcie i wymagają poszukiwania innych modeli i rozwiązań. Po uwagach kierunkowych przedstawiamy rekomendowane przez Izby rozwiązania, w tym działania legislacyjne.

Jako Izba zraszająca przedsiębiorców telekomunikacyjnych, w tym dostawców usługi dostępu do sieci internet, proponujemy dialog i współpracę merytoryczną z Rządem i Szanownymi Paniąmi i Panami Posłami, celem wypracowania rozwiązań, które w sposób racjonalny i sprawiedliwy rozpiszą role i zadania służące ochronie małoletnich przed nieodpowiednimi treściami w internecie, ze szczególnym uwzględnieniem dostępu do treści pornograficznych.

## UWAGI KIERUNKOWE

W ocenie Izby projektowana ustawa wymaga fundamentalnej rekonstrukcji, gdyż projekt w obecnym kształcie budzi szereg bardzo poważnych, kierunkowych i zasadniczych zastrzeżeń, przedstawionych szczegółowo w tej części stanowiska.

### I. Naruszenie prawa Unii Europejskiej i obowiązek notyfikacji Komisji Europejskiej

Projektowana ustawa nakłada na dostawcę usługi dostępu do sieci internet obowiązek zapewnienia trzem kategoriom abonentów<sup>1</sup> możliwość skorzystania z nieodpłatnej usługi ograniczenia dostępu do treści pornograficznych w internecie przez zapewnienie funkcjonalności umożliwiającej blokowanie dostępu do stron internetowych zawierających treści pornograficzne, w sposób przystępny dla abonenta (art. 3 ust. 1 projektowanej ustawy).

Zatem projektowana ustawa wprost nakłada na dostawcę internetu obowiązek blokowania stron internetowych zawierających treści pornograficzne, przy czym obowiązek blokowania ma być realizowany wobec tych abonentów, którzy zażądają takiej usługi. W tym miejscu należy bardzo wyraźnie podkreślić, że obowiązek blokowania stron internetowych zawierających treści pornograficzne jest tożsamy z obowiązkiem monitorowania wszystkich stron internetowych i dostępnych na nich treści, gdyż nie da się zablokować stron internetowych zawierających treści pornograficzne bez wcześniejszego zidentyfikowania takich stron, a zidentyfikowanie takich stron nie jest możliwe bez monitorowania zawartości wszystkich stron dostępnych w internecie. Nie da się oddzielić przysłowiowych plew od ziarna bez przesiania całego ziarna. Biorąc pod uwagę, że Państwo Polskie nie planuje stworzyć rejestru stron zawierających treści pornograficzne, dostawcy internetu nie będą mieli innego sposobu na wywiązanie się z generalnego i ogólnego obowiązku blokowania stron internetowych zawierających treści pornograficzne niż przez monitorowanie (samodzielnie albo zlecając to zadanie podwykonawcom) wszystkich dostępnych w internecie stron internetowych po to, aby najpierw zidentyfikować, a następnie zablokować te z nich, które zawierają treści pornograficzne. Blokowanie wymaga identyfikowania, a identyfikowanie wymaga monitorowania. Obowiązek blokowania jest zatem tożsamy z obowiązkiem monitorowania i identyfikowania treści, które mają być zablokowane.

Z tego właśnie względu przepis prawa nakładający na dostawcę internetu obowiązek blokowania stron internetowych zawierających treści pornograficzne, bez mechanizmu zasilającego dostawców internetu w listę domen do zablokowania, będzie niezgodny z prawem Unii Europejskiej, a bardziej precyzyjnie, taki przepis będzie musiał być uznany za naruszający prawo Unii Europejskiej. Obowiązująca 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) zawiera szereg przepisów o fundamentalnym znaczeniu dla przedsiębiorców telekomunikacyjnych, w tym dostawców usługi dostępu do sieci internet. Pierwszym takim przepisem jest art. 12 dyrektywy o handlu elektronicznym, który określa, w jakich przypadkach dostawca usługi społeczeństwa informacyjnego polegającej na transmisji w sieci telekomunikacyjnej informacji przekazanych przez usługobiorcę lub na zapewnianiu dostępu do sieci telekomunikacyjnej (zwykły przekaz, *mere conduit* w angielskiej wersji językowej), nie ponosi odpowiedzialności za przekazywane informacje. Przepis ten dotyczy przedsiębiorców telekomunikacyjnych (w tym dostawców usługi dostępu do sieci internet) i przewiduje, że przedsiębiorca telekomunikacyjny nie ponosi odpowiedzialności za przekazywane informacje, jeśli i) nie jest inicjatorem przekazu, ii) nie wybiera odbiorcy przekazu oraz iii) nie wybiera oraz nie modyfikuje informacji zawartych w przekazie. Art. 12 dyrektywy o handlu elektronicznym został implementowany do krajowego porządku prawnego przez art. 12 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

---

<sup>1</sup> Osoby fizyczne, osoby fizyczne prowadzące jednoosobową działalność gospodarczą oraz jednostki sektora finansów publicznych prowadzące działalność edukacyjną, opiekuńczą lub wychowawczą względem małoletnich.

W kontekście projektowanej ustawy kluczowe znaczenie ma jednak art. 15 ust. 1 dyrektywy o handlu elektronicznym, który stanowi:

*Państwa Członkowskie nie nakładają na usługodawców świadczących usługi określone w art. 12, 13 i 14 ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność.*

*Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity (w angielskiej wersji językowej dyrektywy)*

Przytoczony przepis jest adresowany do Państw Członkowskich UE i zakazuje Państwom Członkowskim nakładania m.in. na przedsiębiorców telekomunikacyjnych świadczących usługę dostępu do sieci internet ogólnego obowiązku nadzorowania (monitorowania w angielskiej wersji językowej) przekazywanych informacji. Zatem przepisy projektowanej ustawy, nakładające na przedsiębiorcę telekomunikacyjnego świadczącego usługę dostępu do sieci internet generalny, prawny obowiązek blokowania stron internetowych zawierających treści pornograficznych (na żądanie czy też bez żądania abonenta) będą musiały być uznane za przepisy naruszające art. 15 ust. 1 dyrektywy o handlu elektronicznym, gdyż projektowany generalny obowiązek blokowania stron internetowych zawierających treści pornograficzne oznacza również generalny obowiązek nadzorowania (monitorowania) treści internetowych i ich identyfikowanie. A art. 15 ust. 1 dyrektywy o handlu elektronicznym zakazuje Państwom Członkowskim nakładania takiego obowiązku na przedsiębiorców telekomunikacyjnych świadczących usługi dostępu do sieci internet.

Art. 15 ust. 1 dyrektywy o handlu elektronicznym został transponowany do krajowego porządku prawnego przepisem art. 15 ustawy o świadczeniu usług drogą elektroniczną, który stanowi, że 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. W tym miejscu zaznaczyć trzeba, że ewentualne uchylene art. 15 ustawy o świadczeniu usług drogą elektroniczną nie usunie konfliktu projektowanych regulacji z prawem UE, gdyż w dalszym ciągu obowiązuje i będzie obowiązywać adresowany do Państw Członkowskich zakaz wynikający z art. 15 ust. 1 dyrektywy o handlu elektronicznym.

Dyrektywa o handlu elektronicznym zakazuje nakładania obowiązków o charakterze generalnym (ogólnym), a więc zakaz ten nie dotyczy obowiązków o charakterze szczególnym, odnoszących się do konkretnych, indywidualnych spraw. Motyw 47 dyrektyw o handlu elektronicznym stanowi:

*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.*

Przez szczególne przypadki i decyzje władz krajowych, o których mowa w powyżej cytowanym motywie dyrektywy, należy rozumieć rozstrzygnięcia o charakterze indywidualnym (odnoszące się do konkretnej osoby albo organizacji) i konkretnym (odnoszące się do konkretnych okoliczności i stanu faktycznego), a więc przykładowo wyroki sądów oraz decyzje administracyjne. Normy prawne, takie jak przepisy projektowanej ustawy, mają charakter generalny (odnoszą się do wszystkich adresatów spełniających określone kryteria) i abstrakcyjny (nakazane zachowanie jest wymagane od adresata normy w każdym przypadku, gdy ziszcza się określone w normie prawnej przesłanki), zatem statuują obowiązek o charakterze ogólnym (generalnym) i jako takie objęte są zakazem wynikającym z art. 15 ust. 1 dyrektywy o handlu elektronicznym.



Należy podkreślić, że nie ma tu znaczenia fakt, że projektowana ustawa nakłada obowiązek blokowania stron internetowych zawierających treści pornograficzne tym abonentom, którzy zażądali takiej blokady, gdyż z perspektywy dostawcy usługi dostępu do sieci internet złożenie takiego żądania przez jednego choćby abonenta uruchamia generalny i abstrakcyjny obowiązek monitorowania, identyfikowania i blokowania stron internetowych zawierających treści pornograficzne na rzecz wszystkich abonentów, którzy takie żądanie zgłosili.

W tym miejscu należy zaznaczyć, że na poziomie UE zakończyły się prace legislacyjne nad Aktem o Usługach Cyfrowych<sup>2</sup>, a dokument ten został ogłoszony w Dzienniku Urzędowym Unii Europejskiej<sup>3</sup>. Piszemy o tym, gdyż Akt o Usługach Cyfrowych uchyla analizowane powyżej art. 12 – 15 dyrektywy o handlu elektronicznym, a treść tych przepisów zostaje inkorporowana do tekstu Aktu o Usługach Cyfrowych, w ten sposób, że w analizowanym zakresie nie zajdą zmiany w prawie UE wraz z wejściem w życie Aktu o Usługach Cyfrowych. Następcą art. 12 dyrektywy o handlu elektronicznym jest art. 3 Aktu o Usługach Cyfrowych, który przewiduje takie same przesłanki wyłączenia odpowiedzialności przedsiębiorcy telekomunikacyjnego świadczącego usługę dostępu do sieci internet. Natomiast następcą art. 15 dyrektywy o handlu elektronicznym, zakazującego Państwu Członkowskim nakładania ogólnego obowiązku w zakresie monitorowania treści, jest art. 8 Aktu o Usługach Cyfrowych, który stanowi:

***Brak ogólnych obowiązków w zakresie monitorowania lub aktywnego ustalania faktów***

*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.*

***No general monitoring or active fact-finding obligations***

*No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers.*

Akt o Usługach Cyfrowych jest rozporządzeniem, a więc aktem prawa UE który będzie miał bezpośrednie zastosowanie na terytorium Państw Członkowskich UE, co oznacza, że uchylone będą musiały być obecnie obowiązujące przepisy art. 12 – 15 ustawy o świadczeniu usług drogą elektroniczną, ze względu na uregulowanie tej materii w Akcie o Usługach Cyfrowych.

Z informacji pozyskanych podczas prac rządowych nad projektowaną ustawą wynika, że przepisy projektowanej ustawy nie były przedmiotem oceny zgodności z prawem Unii Europejskiej, realizowanej przez Ministra do Spraw Unii Europejskiej. Ze względu na fakt, że projektowana ustawa nie jest aktem prawnym implementującym do krajowego porządku prawnego przepisy prawa UE Minister do Spraw Unii Europejskiej na etapie prac rządowych nie przeprowadził takiej oceny z urzędu (gdyż w takim przypadku, zgodnie z regulaminem prac Rady Ministrów, nie jest do tego zobowiązany), a jednocześnie, pomimo naszych próśb, Minister Cyfryzacji (Projektodawca) nie zdecydował się na wystąpienie do Ministra do Spraw Unii Europejskiej z wnioskiem o przeprowadzenie takiej oceny.

Ponadto, w ocenie Izby projektowana ustawa podlega obowiązkowi notyfikacji na zasadach określonych w rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (rozporządzenie w sprawie notyfikacji), którego przepisy implementują i wykonują w ramach krajowego porządku prawnego dyrektywę 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (dyrektywa

---

<sup>2</sup> 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).

<sup>3</sup> <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022R2065&qid=1666867747437&from=EN>

w sprawie zasad dotyczących usług społeczeństwa informacyjnego)<sup>4</sup>. Dyrektywa ta nakłada na Państwa Członkowskie obowiązek przekazania Komisji Europejskiej wszelkich projektów przepisów technicznych, z wyjątkiem tych, które w pełni stanowią transpozycję normy międzynarodowej lub europejskiej, w którym to przypadku wystarczająca jest informacja dotycząca odpowiedniej normy (art. 5 ust. 1 dyrektywy w sprawie zasad dotyczących usług społeczeństwa informacyjnego). Przez „przepisy techniczne” dyrektywa każe rozumieć: *specyfikacje techniczne i inne wymagania bądź zasady dotyczące usług, włącznie z odpowiednimi przepisami administracyjnymi, których przestrzeganie jest obowiązkowe, de jure lub de facto, w przypadku wprowadzenia do obrotu, świadczenia usługi, ustanowienia operatora usług lub korzystania w państwie członkowskim lub na przeważającej jego części, jak również przepisy ustawowe, wykonawcze i administracyjne państw członkowskich, z wyjątkiem określonych w art. 7, zakazujące produkcji, przywozu, wprowadzania do obrotu lub stosowania produktu lub zakazujące świadczenia bądź korzystania z usługi lub ustanawiania dostawcy usług* (art. 1 ust. 1 lit. f) dyrektywy w sprawie zasad dotyczących usług społeczeństwa informacyjnego). Natomiast przez „usługę”, której mają dotyczyć przepisy techniczne, należy rozumieć każdą usługę społeczeństwa informacyjnego, to znaczy każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług (art. 1 ust. 1 lit. b) dyrektywy w sprawie zasad dotyczących usług społeczeństwa informacyjnego). Unijne definicje i wymagania mają swoje odpowiedniki w rozporządzeniu w sprawie notyfikacji, które w sposób tożsamy do wcześniej przytoczonej dyrektywy definiuje „przepisy techniczne” (§ 2 pkt 5) rozporządzenia) oraz „usługę” (§ 2 pkt 1 rozporządzenia) oraz stanowi o obowiązku notyfikacji aktów prawnych zawierających przepisy techniczne (§ 4 rozporządzenia). W przypadku usług społeczeństwa informacyjnego celem procedury notyfikacji projektu aktu prawnego do Komisji Europejskiej jest ocena, czy projektowane regulacje nie naruszają przepisów prawa UE, a w szczególności przepisów prawa UE, które gwarantują swobodny przepływ usług społeczeństwa informacyjnego w ramach rynku wewnętrznego (patrz art. 3 ust. 2 dyrektywy o handlu elektronicznym, który stanowi: *Państwa Członkowskie nie mogą z powodów wchodzących w zakres koordynowanej dziedziny ograniczać swobodnego przepływu usług społeczeństwa informacyjnego pochodzących z innego Państwa Członkowskiego*).

Bez względu na ocenę moralną i społeczną dostarczania treści pornograficznych (z wyłączeniem treści i zachowań nielegalnych takich jak pornografia dziecięca czy zoofilia) dostarczanie treści pornograficznych, jeśli odbywa się za pośrednictwem sieci internet, co do zasady będzie stanowiło usługę społeczeństwa informacyjnego w rozumieniu dyrektywy w sprawie zasad dotyczących usług społeczeństwa informacyjnego oraz rozporządzenia. A więc przepisy projektowanej ustawy, nakazujące blokowanie stron internetowych zawierających treści pornograficzne, stanowią projekt przepisów technicznych w rozumieniu ww. przytoczonej dyrektywy i rozporządzenia, gdyż zawierają przepisy prawa (nakaz blokowania) bezpośrednio wpływające i ograniczające możliwość świadczenia tego typu usług społeczeństwa informacyjnego na terytorium RP, pochodzących z innych Państw Członkowskich UE (rynek wewnętrzny). Zatem projektowana ustawa objęta jest obowiązkiem notyfikacji na zasadach określonych rozporządzenie w sprawie notyfikacji.

Zaznaczyć należy, że w tym przypadku nie znajduje zastosowania przepis przytoczonego rozporządzenia, który wprowadza wyjątek od obowiązku notyfikacji dla projektów aktów prawnych dotyczących usług telekomunikacyjnych objętych zakresem regulacji prawa Wspólnoty Europejskiej (§ 4 ust. 2 pkt 1 rozporządzenia). Podobny, ale nie tożsamy (bo o węższym zakresie zastosowania) wyjątek od obowiązku notyfikacji przewiduje powołana dyrektywa dla zasad odnoszących się do zagadnień objętych przepisami Unii w dziedzinie usług telekomunikacyjnych, o których mowa w dyrektywie Parlamentu Europejskiego i Rady 2002/21/WE (po zmianach należy to odesłanie czytać jako odesłanie do europejskiego Kodeksu łączności elektronicznej). Wyjątek ten nie znajduje zastosowania w przypadku projektowanej ustawy, gdyż:

---

<sup>4</sup> Dyrektywa ta uchyliła i zastąpiła dyrektywę 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiająca procedurę udzielania informacji w zakresie norm i przepisów technicznych.

- projektowana ustawa przewiduje obowiązki, które nie są objęte zakresem regulacji prawa Unii Europejskiej (nie ma przepisów prawa UE, które nakładałyby na przedsiębiorców telekomunikacyjnych generalny obowiązek blokowania treści pornograficznych);
- wymóg notyfikowania projektowanej ustawy wynika nie tyle z faktu nakładania obowiązków na przedsiębiorców telekomunikacyjnych, co z tego, że obowiązek ten ma bezpośredni wpływ na swobodę przepływu usług świadczonych drogą elektroniczną na rynku wewnętrznym Unii Europejskiej.

W ocenie Izby projekt ustawy powinien być notyfikowany ze względu na przepisy techniczne mające znacznie dla rynku wewnętrznego UE. Brak takiej notyfikacji przed skierowaniem projektowanej ustawy do prac w Sejmie powoduje, że wątpliwości dotyczące zgodności projektowanej ustawy z prawem UE będą towarzyszyły projektowanej ustawie do końca prac legislacyjnych, narażając Polskę na postępowanie w sprawie naruszenia prawa UE po uchwaleniu ustawy.

Podsumowując tę część wyводу:

1. przyjęcie projektowanej ustawy w obecnym kształcie będzie stanowiło naruszenie art. 15 ust. 1 dyrektywy o handlu elektronicznym (w przyszłości art. 7 Aktu o Usługach Cyfrowych);
2. projekt ustawy przed uchwaleniem powinien być notyfikowany Komisji Europejskiej zgodnie z przepisami rozporządzenia w sprawie notyfikacji.

## **II. Obowiązujące przepisy prawa oraz waga wychowania i edukacji**

Projektowana ustawa jest przykładem podejścia, które zakłada, że każdy problem społeczny należy i da się rozwiązać za pomocą nakazów i zakazów ustawowych. Jest to przeświadczenie błędne, gdyż nie da się rozwiązywać skomplikowanych problemów społecznych wyłącznie nakazami i zakazami prawnymi, takie działanie jest atrakcyjne wyłącznie politycznie i medialnie, bo wydaje się oferować proste rozwiązania dla skomplikowanych problemów. Jednym z efektów jest to, że tworzone są ustawy, które nie przynoszą zamierzonego efektu społecznego, a reakcją na brak rezultatów są kolejne nowelizacje, nowe nakazy i zakazy, nakładanie kolejnych warstw przepisów. Końcowym efektem jest obserwowana w Polsce inflacja prawa - każdego roku polski Prawodawca tworzy więcej stron przepisów prawa niż rok wcześniej, a skutkiem jest komplikowanie otoczenia prawnego, w którym muszą funkcjonować obywatele i przedsiębiorcy.

Rząd i Państwo Polskie, identyfikując faktyczny problem społeczny, jakim jest zbyt łatwy dostęp do treści pornograficznych przez osoby niepełnoletnie, powinno w pierwszym kroku zastanowić się, jakie działania poza-legislacyjne można podjąć, aby problem ten zaadresować. Dopiero jeśli analiza taka wykaże, że problemu nie da się rozwiązać narzędziami poza-legislacyjnymi należałoby się zastanowić, jak usprawnić egzekucję albo poprawić obowiązujące już przepisy prawa. Tworzenie nowych ustaw i obszarów regulowanych powinno być traktowane jako ostateczność, gdy wszystkie inne rozwiązania zawiodą. Analiza projektowanej ustawy, uzasadnienia oraz Oceny Skutków Regulacji nie daje podstaw do sądenia, że takie analizy i działania były podejmowane zanim zdecydowano się na przygotowanie radykalnego w swoich założeniach projektu ustawy.

Zgodnie z zaprezentowaną logiką prawidłowego działania w pierwszej kolejności należałoby się skupić na analizie możliwości rozwiązania problemu poprzez działania poza-legislacyjne, takie jak działania wychowawcze, edukacyjne i informacyjne, skierowane zarówno do rodziców i dzieci, w tym działania informujące i promujące wykorzystanie przez rodziców istniejących już rozwiązań technicznych wspierających ochronę dzieci przed zagrożeniami świata wirtualnego. W dyskursie publicznym eksperci podkreślają, że o ile rozwiązania techniczne są pomocne (i są już dzisiaj dostępne) to nie zastąpią one uwagi i rozmowy rodzica z dzieckiem, edukacji i informacji na temat istniejących zagrożeń jak i sposobów radzenia sobie z nimi. Wychowywanie dzieci jest bez wątpienia rolą nas, rodziców, natomiast systemowa



edukacja i informacja to bez wątpienia zadanie Państwa Polskiego, a projektowana ustawa zmierza do „przerzucenia” odpowiedzialności za informację i edukację na przedsiębiorców telekomunikacyjnych. Należy jeszcze raz stanowczo podkreślić, że edukowanie społeczeństwa jest rolą Państwa Polskiego, a przedsiębiorcy mogą wspierać działania Państwa w tym zakresie, ale nie mogą Państwa zastąpić lub wyręczyć.

A jest o czym edukować i o czym informować. Z jednej strony należy edukować i informować, rodziców i dzieci, o zagrożeniach jakie stwarza świat cyfrowy, gdzie dostęp małoletnich do treści pornograficznych jest jednym z wielu zagrożeń i problemów. Osoba nieświadoma zagrożeń nie będzie rozumiała potrzeby ochrony siebie i swoich bliskich. Osobom świadomym zagrożeń należy przekazywać wiedzę i informację o tym, jak radzić sobie z tymi zagrożeniami. A rozwiązania techniczne to tylko wycinek tego, co można zrobić aby chronić siebie i bliskich, a najważniejsze wcale nie są takie czy inne rozwiązania techniczne, ale wyrobienie w sobie i bliskich odpowiednich wzorców zachowań i nawyków. A jeśli już o rozwiązaniach technicznych mowa to tych jest bardzo dużo, są rozwiązania odpłatne, są rozwiązania darmowe, zarówno takie, które są bardzo proste w obsłudze jak i takie, które wymagają większego zaangażowania. Są to rozwiązania dostępne już teraz dla każdego, kto chce z nich korzystać. Nie ma potrzeby w tym miejscu opisywać poszczególnych dostępnych rozwiązań, ale żeby nie być posądzonym o gołosłowność wskazujemy, że swojego rodzaju inwentaryzację dostępnych rozwiązań technicznych, wraz z przystępnymi tutorialami wideo pokazującym krok po kroku jak tych narzędzi korzystać, przygotowało i udostępniło Stowarzyszenie Twoja Sprawa<sup>5</sup>, organizacja od lat zajmująca się problematyką ochrony dzieci przed dostępem do treści pornograficznych w internecie. Dostępne już dzisiaj narzędzia Stowarzyszenie Twoja Sprawa pogrupowało w sześć kategorii:

- zabezpieczenia oferowane przez operatorów sieci komórkowych;
- zabezpieczenia na telefony z systemem Android i iOS;
- aplikacje zewnętrzne;
- OpenDNS;
- narzędzia ochrony rodzicielskiej wbudowane w system Windows;
- rozwiązania oferowane przez dostawców internetu (stacjonarnego);

Przy czym należy pamiętać, że pod niektórymi kategoriami kryje się po kilka narzędzi, a więc łącznie mamy do czynienia z kilkunastoma narzędziami do ochrony dzieci przed zagrożeniami świata wirtualnego. Katalog ten należy uzupełnić o aplikację mOchrona, czyli narzędzie kontroli rodzicielskiej stworzone z wykorzystaniem środków publicznych przez NASK i dostępne publicznie dla każdego, za darmo<sup>6</sup>.

Istniejące już rozwiązania techniczne mają dwie przewagi nad projektowaną ustawą:

- są dobrowolne, co może brzmieć jak oczywista oczywistość, ale dzięki temu, że nie są związane z ustawowym, generalnym obowiązkiem blokowania, nie występuje konflikt z prawem Unii Europejskiej;
- istniejące rozwiązania zapewniają znacznie szerszą ochronę niż rozwiązanie ustawowe, które (przynajmniej na razie, patrz kolejne uwagi) skupia się na ochronie przed dostępem do treści pornograficznych; wiele z istniejących rozwiązań chroni nie tylko przed treściami pornograficznymi ale również przed innymi treściami, które są uznawane za szkodliwe; ponadto, narzędzia takie oferują często znacznie szerszy wachlarz funkcjonalności, niż tylko kontrola treści, pozwalając np. kontrolować czas jaki dziecko spędza przed ekranem czy ilość czasu, jaką poświęca na granie czy korzystanie z konkretnych aplikacji lub usług, dając rodzicowi nie tylko wgląd, ale i kontrolę nad niemal wszystkimi aspektami aktywności dziecka w świecie cyfrowym.

<sup>5</sup> <https://twojasprawa.org.pl/article/narzedzia-ochrony-rodzicielskiej-poradnik>

<sup>6</sup> <https://www.nask.pl/pl/aktualnosci/4365,Aplikacja-mOchrona-stworzona-dla-rodzicow-z-mysla-o-dzieciach.html>

W ocenie Izby zidentyfikowane przez Projektodawcę problemy mogą i powinny zostać rozwiązane z wykorzystaniem działań nie władczych, a zaprojektowana regulacja nie spełnia wymogu proporcjonalności i adekwatności.

W debacie publicznej często pada argument, powtórzony zresztą w uzasadnieniu do projektowanej ustawy, że zbyt mało rodziców korzysta z już istniejących rozwiązań, co jest tłumaczone brakiem czasu, zainteresowania, wiedzy lub świadomości o zagrożeniach i kompetencji niezbędnych do korzystania z istniejących narzędzi. Na brak czasu lub zainteresowania niewiele można poradzić, ale poziom świadomości i kompetencji z pewnością można poprawić odpowiednimi kampaniami informacyjnymi i edukacyjnymi, które powinny być realizowane przez instytucje publiczne odpowiedzialne za politykę społeczną i rodzinną (Ministerstwo Rodziny i Polityki Społecznej wspólnie z funkcjonującą w jego ramach Radą Rodziny), ochronę praw dzieci (Rzecznik Praw Dziecka), dbanie o bezpieczeństwo komunikacji elektronicznej (Prezes Urzędu Komunikacji Elektronicznej), edukację (Ministerstwo Edukacji i Nauki, szkoły i nauczyciele), przy wsparciu mediów realizujących misję publiczną (publiczna telewizja i radio). Na przestrzeni ostatnich lat Państwo Polskie z powodzeniem realizuje, z wykorzystaniem środków publicznych, przeróżne kampanie promocyjne i informacyjne, jak choćby te zachęcające do szczepień przeciwko COVID-19, informujące o korzyściach płynących z kolejnych Tarcz, czy zachęcających do skorzystania z tzw. wakacji kredytowych. W dokumentach towarzyszących projektowanej ustawie nie ma nawet wzmianki o tym, że takie kampanie informacyjne są planowane czy że choć były rozważane. Trudno jest zrozumieć, czemu Państwo Polskie nie chce albo nie może podjąć się takich działań w kwestii ochrony dzieci przed dostępem do nieodpowiednich treści patrząc na skalę publicznych akcji promocyjnych w innych obszarach aktywności Państwa.

Podsumowując, Państwo Polskie powinno zaangażować się w działania edukacyjne, informacyjne i uświadamiające na temat istniejących zagrożeń i sposobów na radzenie sobie z nimi.

Jednocześnie Państwo Polskie powinno dokonać przeglądu istniejących przepisów prawa i zastanowić się co można zrobić, aby były one skuteczniej egzekwowane. W dokumentach towarzyszących projektowanej ustawie próżno szukać informacji, aby takie analizy były prowadzone, a jeśli były, to jakie wnioski płyną z takiej analizy. W ustawie – Kodeks karny funkcjonują już przepisy, których celem jest ochrona małoletnich przed dostępem do treści pornograficznych. Art. 200 § 3 - 5 Kodeksu karnego stanowią:

*§ 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.*

Jak widać więc funkcjonują już przepisy prawa, których *ratio legis* jest ochrona małoletnich przed treściami o charakterze pornograficznym. Pytaniem, na które nie znajdujemy odpowiedzi w publikowanych kolejnych wersjach projektu ustawy i jej uzasadnieniu, jak i w innych dokumentach przedstawianych w ramach rządowego etapu procesu legislacyjnego, jest to, czemu Projektodawca uznał, że wyżej przytoczone przepisy są niewystarczające i czemu nie skupiono się na próbie poprawienia egzekucji albo zmiany tego przepisu tak, aby egzekucja była możliwa.

Przy tej okazji zwracamy uwagę, że przytoczone przepisy Kodeksu karnego, inaczej niż projektowana ustawa, odpowiedzialnymi za prezentowanie treści pornograficznych małoletniemu czynią dostawców tych treści. Jednym z najpoważniejszych wad projektowanej ustawy jest to, że w sposób nieuzasadniony i zwyczajnie niesprawiedliwy przenosi odpowiedzialność za treści pornograficzne z dostawców tych treści

na dostawców usługi dostępu do sieci internet. Wręcz uderzające jest, że projekt ustawy nie zawiera absolutnie żadnych przepisów, zakazów i nakazów adresowanych wobec dostawców treści pornograficznych, a więc w najmniejszym choć stopniu nie dotyka i nie odnosi się do źródła problemu. Z projektowanej ustawy wynika, że kar związanych z treściami pornograficznymi, nakładanych przez ministra właściwego do spraw informatyzacji, będą musieli obawiać się wyłącznie przedsiębiorcy telekomunikacyjni, podczas gdy dostawcy treści pornograficznych będą mogli „spać spokojnie”. Projektodawca nie widzi dla siebie żadnej roli w eliminowaniu problemu i nie widzi potrzeby nakładania żadnych obowiązków administracyjnych na dostawców treści pornograficznych, zarówno tych krajowych jak i zagranicznych. Rozwiązanie, które odpowiedzialność i ryzyko kar pieniężnych związanych z treściami pornograficznymi składa w całości na barki przedsiębiorców telekomunikacyjnych, które jednocześnie nie nakłada absolutnie żadnych ograniczeń czy wymagań na krajowych i zagranicznych dostawców treści pornograficznych, ograniczające rolę państwa do recenzowania skuteczności wysiłków dostawców internetu, jest niesprawiedliwe.

Wracając do przepisów art. 200 § 3 - 5 Kodeksu karnego to domyślamy się, że poważnym ograniczeniem w ich stosowaniu mogą być trudności w pociągnięciu do odpowiedzialności osób przebywających poza granicami kraju. Jeśli tak, to zastanowić się trzeba, jak ten problem zaadresować i wydaje się, że odpowiedź jest zawarta w OSR do projektu ustawy, gdzie Projektodawca opisał (ale nie zdecydował się skorzystać) rozwiązania wdrożone w Niemczech i we Francji, wdrażane w Wielkiej Brytanii. Z OSR wynika, że w Niemczech i Francji został wdrożony model regulacyjny, który od dostawców treści pornograficznych wymaga wdrożenia skutecznych mechanizmów weryfikacji wieku użytkowników (tak, aby odmówić dostępu osobie niepełnoletniej), a jeśli dostawca (z kraju albo z zagranicy) nie wywiązuje się z tego obowiązku to właściwy organ państwa, po stwierdzeniu takiego faktu, wpisuje domenę takiego dostawcy na specjalną listę, a następnie dostawcy internetu blokują dostęp do takich stron na poziomie DNS. Koncepcję tą rozwiniemy szerzej w dalszej części niniejszego stanowiska, niemniej już w tym miejscu widać, że model wdrożony w Niemczech i we Francji wpisywałby się lepiej w polski porządek prawny i byłby efektywniejszy niż model zaproponowany w projektowanej ustawie. Nałożenie na dostawców treści pornograficznych obowiązku skutecznej weryfikacji wieku stanowiłoby bowiem naturalny dalszy krok w realizacji *ratio legis*, jakie przyświecało wprowadzeniu art. 200 § 3 - 5 Kodeksu karnego, a jednocześnie w bardzo łatwy i skuteczny sposób można by wykorzystać istniejący na podstawie ustawy o grach hazardowych rejestr blokowanych domen do blokowania tych domen, na których dostępne są treści pornograficzne bez skutecznej weryfikacji wieku. Trzeba również pamiętać, że w dyskursie publicznym od lat pojawia się projekt ustawy wspomnianego już Stowarzyszenia Twoja Sprawa, którego główne założenia są zbliżone do modelu wdrożonego w Niemczech i we Francji i wdrażanego w Wielkiej Brytanii. Tym bardziej niezrozumiałe jest, czemu Projektodawca, dysponując wiedzą o wdrożonych i sprawdzonych modelach funkcjonujących już w innych państwach Europy, kierunkowo wspieranych przez organizacje społeczne zajmujące się ochroną dzieci przed pornografią, zdecydował się na rozwiązanie całkowicie odmienne, które być może nie zostało wdrożone w żadnym innym państwie na świecie, a przynajmniej brak jest informacji o tym, aby jakiegokolwiek inne państwo zdecydowało się na model zaproponowany w projektowanej ustawie.

Podsumowując tę część stanowiska:

1. widzimy potrzebę zainicjowania i prowadzenia przez Państwo Polskie dedykowanych kampanii edukacyjno – informacyjnych na temat zagrożeń i sposób radzenie sobie z zagrożeniami świata cyfrowego, na wzór prowadzonych przez Państwo Polskie kampanii promocyjnych w innych obszarach;
2. dostrzegamy potrzebę przeprowadzenia pogłębionych analiz istniejących już przepisów prawa; jeśli w efekcie takich analiz ustalone zostanie, że nie jest możliwe podniesienie skuteczności egzekucji obowiązujących już przepisów należy rozważyć wprowadzenie nowych rozwiązań prawnych, wzorowanych na rozwiązaniach wdrożonych w Niemczech i we Francji i wdrażanych w Wielkiej Brytanii, z możliwie szerokim wykorzystaniem istniejących już przepisów prawa (Kodeks

karny) i rozwiązań technicznych (rejestr blokowanych domen działający na podstawie ustawy o grach hazardowych).

### III. Złudne poczucie bezpieczeństwa

Na stronach Ministerstwa Cyfryzacji można przeczytać m.in.<sup>7</sup>:

*Rządowy projekt daje rodzicom proste i dobrowolne narzędzie do blokowania dostępu do treści pornograficznych. Wystarczy, że zwrócą się o to do swojego operatora telekomunikacyjnego, a on uruchomi odpowiednią blokadę. Takie przepisy są potrzebne, ponieważ nie każdy rodzic posiada biegłość w instalacji programów ograniczających dzieciom dostęp do niepożądanych treści. Po wejściu w życie nowego prawa, te umiejętności nie będą potrzebne. Aż tyle i tylko tyle.*

Projektowana ustawa, jak również towarzyszące jej wypowiedzi medialne, sugerujące, że rodzice już nic nie będą musieli robić poza zgłoszeniem żądania do dostawcy usługi dostępu do sieci internet tworzą złudne, poczucie bezpieczeństwa. Złudne z co najmniej dwóch powodów:

1. każde rozwiązanie techniczne ma swoje ograniczenia, żadne nie gwarantuje 100% skuteczności blokowania;
2. każde rozwiązanie techniczne przy odrobinie determinacji i podstawowej wiedzy (dostępnej powszechnie w internecie) da się ominąć.

Jeśli chodzi o rozwiązania w praktyce dostępne z poziomu sieci telekomunikacyjnych to dostawy usług dostępu do sieci internet mają możliwość blokowania stron internetowych zawierających treści pornograficzne poprzez blokowanie na poziomie serwerów DNS domen wykorzystywanych do udostępniania lub rozpowszechniania treści pornograficznych, czyli w sposób, który już obecnie jest wykorzystywany do blokowania domen służących do oferowania gier hazardowych niezgodnie z ustawą (art. 15f ustawy z dnia 19 listopada 2009 r. o grach hazardowych), przy czym należy jednoznacznie podkreślić, że nie istnieją rozwiązania techniczne, które gwarantują 100% procentową skuteczność w blokowaniu treści pornograficznych czy dowolnych innych, a jednocześnie zawsze jest ryzyko, że zablokowane zostaną treści nie będące treściami pornograficznymi (*false positive*). Każde zabezpieczenie techniczne da się ominąć, przy odrobieniu determinacji i wiedzy, która jest powszechnie dostępna w internecie, a zasadą jest, że młodzi radzą sobie z rozwiązaniami cyfrowymi znacznie lepiej niż ich rodzice i opiekunowie. Wszystko to powoduje, że o ile rozwiązania techniczne są przydatne i pomocne w ochronie dzieci, to nie rozwiązują wszystkich problemów i nigdy nie zastąpią rozmowy i uwagi poświęconej dziecku przez rodzica.

Naturalnie można zadać pytanie, czemu piszemy o tym w stanowisku, skoro techniczne ograniczenia i możliwość ominięcia zabezpieczeń dotyczą nie tylko projektowanej blokady ustawowej, ale również dostępnych już dzisiaj rozwiązań technicznych. Podnosimy tę kwestię, gdyż wraz prowadzeniem prawnego obowiązku blokowania, którego realizacja ma być zagrożona administracyjną karą pieniężną, diametralnie zmienia się otoczenie regulacyjne i znaczenie prawne obiektywnie istniejących ograniczeń i uwarunkowań technicznych. Zakres i zasady działania dzisiaj dostępnych usług i mechanizmów blokowania, w tym zakres ich niedziałania i ograniczenia techniczne, to przedmiot umowy (regulaminu) jaką z dostawcą rozwiązania zawiera osoba, która chce z danego narzędzia korzystać. Jeśli rodzic akceptuje określone zasady działania rozwiązania, którym jest zainteresowany, to akceptuje regulamin usługi, zawiera umowę z dostawcą i korzysta z narzędzia. Jeśli narzędzie nie spełnia oczekiwań klienta, to klient może zrezygnować z niego i zacząć korzystać z innego narzędzia. Wszelkie ograniczenia i uwarunkowania działania dostępnych dzisiaj narzędzi to kwestia umowy, a więc woli stron. Projektowana ustawa to diametralnie odmienna sytuacja, gdyż skuteczność blokady, którą dostawca internetu ma realizować na rzecz abonenta, będzie oceniana,

<sup>7</sup> <https://www.gov.pl/web/cyfryzacja/List-Ministra-Janusza-Cieszynskiego-do-Pani-Katarzyny-Kozlowskiej-Redaktor-Naczelnej-Fakt>

pod groźbą kary za nieskuteczność, minister właściwy do spraw informatyzacji. Dla pełnego obrazu sytuacji dodać trzeba, że projekt ustawy zawiera również przepis, który nakłada na dostawców usługi dostępu do sieci internet obowiązek wdrożenia i zapewnienia odpowiednich środków technicznych i organizacyjnych w celu realizacji obowiązku blokowania stron internetowych zawierających treści pornograficzne, uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz skuteczność przyjętego rozwiązania (art. 3 ust. 2 projektu ustawy). Przepis ten odczytujemy w ten sposób, że dostawca usługi dostępu do sieci internet będzie mógł wdrożyć takie rozwiązania blokujące strony internetowe zawierające treści pornograficzne, które zapewnią, że blokada będzie na tyle skuteczna, na ile z jednej strony pozwala rozwój technologiczny a z drugiej strony na ile pozwala budżet i sytuacja ekonomiczna dostawcy. Bez wątplenia tego typu przepis, racjonalizujący zakres obowiązku, jest krokiem w dobrym kierunku, niemniej jednak nie usuwa całkowicie obaw związanych ze znacznym zakresem uznaniowości, jakim będzie dysponował Minister oceniając czy dostawcy usługi dostępu do sieci internet prawidłowo wywiążą się z obowiązków wynikających z ustawy.

Rozważając na temat tworzenia fałszywego poczucia bezpieczeństwa nie można zapominać, że projektowana ustawa dotyczy blokowania treści pornograficznych, a przecież nie jest to jedyna kategoria treści jaka może być szkodliwa dla małoletnich, a treści to tylko jedno z wielu zagrożeń świata cyfrowego, których projektowana ustawa nie adresuje. Tym bardziej projektowana ustawa nie powinna być traktowana i prezentowana społeczeństwu jako „załatwienie” wszystkich problemów z bezpieczeństwem dzieci w świecie cyfrowym.

Abstrahując od uwarunkowań i ograniczeń technologicznych należy być świadomym, że projektowana ustawa i wymóg kwalifikacji stron internetowych jako zawierających albo niezawierających treści pornograficznych, na potrzeby obejmowania albo nieobjmowania takich stron ustawową blokadą, będzie generowała liczne spory na linii abonent – dostawca treści – dostawca dostępu do internetu, co do tego, czy dana strona i treść została prawidłowo zakwalifikowana. Spory, w których rozpatrywanie będą zaangażowani abonenci, przedsiębiorcy telekomunikacyjni, podmioty administrujące stronami internetowymi, dostawcy treści wyświetlanych na stronach, ale również organy państwa i wreszcie sądy powszechne.

Podsumowując, uważamy, że przyszłe rozwiązania w tym zakresie powinny być tworzone na wzór albo wręcz w oparciu o sprawdzone już rozwiązania, wdrożone na potrzeby blokowania domen służących do oferowania gier hazardowych niezgodnie z ustawą o grach hazardowych. Ponadto uważamy, że projektowana ustawa, jak również używana debacie publicznej argumentacja, nie powinna sugerować, że wystarczy, aby abonent zażądał usługi i „sprawa załatwiona”, gdyż budowanie takiej narracji może doprowadzić do wytworzenia nieprawdziwego i szkodliwego przeświadczenia zarówno po stronie rodziców, decydentów i mediów, że nic już nie trzeba robić, bo ustawa zapewnia bezpieczeństwo dzieci w świecie cyfrowym.

#### **IV. Obowiązki dostawców treści pornograficznych**

Nie sposób jest zaakceptować ustawę, która ma chronić przed treściami pornograficznymi a jednocześnie w żaden sposób nie jest adresowana do dostawców treści pornograficznych. Z niezrozumiałych powodów Projektodawca zdecydował, że wszystkie obowiązki związane z ochroną małoletnich przed treściami pornograficznymi będą ciążyły nie na dostawcach tych treści, a na przedsiębiorcach telekomunikacyjnych świadczących usługę dostępu do sieci internet, którzy nie mają nic wspólnego z treściami pornograficznymi, tak jak nie zajmują się jakąkolwiek inną kategorią treści. To trochę tak, jakby za sprzedaż przez sklepy dla dorosłych treści pornograficznych małoletnim odpowiedzialnością obarczać firmy transportowe i spedycyjne, które przewożą towary do wszystkich sklepów i punktów usługowych, w tym do sklepów dla dorosłych.



Rolą i istotą działalności przedsiębiorców telekomunikacyjnych, w tym dostawców usługi dostępu do sieci internet, jest zapewnienie łączności, a więc przekazanie informacji (dowolnej) od nadawcy do odbiorcy tej informacji. Treść to domena dostawców treści. Nie rozumiemy jakimi kryteriami kierował się Projektodawca tworząc projekt ustawy, który ma chronić małoletnich przed pornografią, a w całości pomija rolę i odpowiedzialność dostawców treści pornograficznych. Co gorsze, Projektodawca uznał, że nie tylko odpowiedzialność za treści należy przenieść z dostawców treści na dostawców łączności, gdyż również zadania Państwa Polskiego, takie jak działania informacyjne mają być realizowane przez dostawców łączności. Można by zażartować, że celem Projektodawcy były skupienie wszystkich kompetencji i odpowiedzialności za treści pornograficzne w rękach przedsiębiorców telekomunikacyjnych, ale byłby to ponury żart, biorąc pod uwagę ryzyko drakońskich kar, jakie wiążą się z takim „wyróżnieniem”.

Jeśli zaproponowany kierunek wynika tylko i wyłącznie z tego, że dostawcy treści pornograficznych to nie tylko podmioty krajowe, ale i zagraniczne, a więc takie, do których nie sięga jurysdykcja Państwa Polskiego, a przedsiębiorcy telekomunikacyjni mają siedziby w kraju i łatwo nałożyć na nie obowiązki i regulacje, to takie uzasadnienie nie może zostać zaakceptowane. Bez wątplenia istnieją obiektywne trudności w wyegzekwowaniu krajowych regulacji wobec podmiotów działających poza granicami kraju, ale po pierwsze nie jest to powód, aby obowiązkami obciążać podmioty krajowe, a po drugie istnieją konstrukcje i mechanizmy, które pomagają rozwiązać problem jurysdykcji i egzekucji. Przede wszystkim zwracamy uwagę, że rozwiązania wdrożone w Niemczech, Francji i wdrażane w Wielkiej Brytanii prawidłowo adresują obowiązki, nakładając obowiązek skutecznego weryfikowania wieku użytkownika na dostawców treści pornograficznych. A w przypadku, gdy dostawca treści nie wywiązuje się z tak określonego obowiązku, to domena takiego dostawcy decyzją uprawnionego organu państwa jest wpisywana do rejestru, a domeny wciągnięte do takiego rejestru są blokowane przez działających w tych krajach dostawców internetu. Rozwiązanie takie usuwa problemy związane z egzekwowaniem prawa poza granicami, bowiem nie trzeba takiego prawa egzekwować poza granicami, wystarczy uznać, że dostawca treści nie wywiązał się z obowiązków wynikających z prawa krajowego, a sankcją jest zablokowanie dostępności domeny takiego dostawcy na terytorium danego kraju. Jak widać więc, można stworzyć mechanizm, który prawidłowo adresuje obowiązki na dostawców treści pornograficznych, rezerwując dla dostawców internetu rolę wspierającą, polegającą na blokowaniu domen tych dostawców treści, którzy nie wywiązują się ze swoich obowiązków.

Podsumowując, ustawa, która ma na celu ochronę dzieci przed treściami pornograficznymi, nie może pomijać roli i odpowiedzialności dostawców treści pornograficznych i przenosić całą odpowiedzialność za te treści na dostawców łączności.

## V. Otwarty internet

Internet był siecią prawdziwie otwartą na początku swojego funkcjonowania, zaraz po opuszczeniu laboratoriów i ośrodków akademickich, a w miarę jak trafiał pod tzw. strzechy prawodawcy zaczęli stopniowo rozumieć skalę i znaczenie tego fenomenu i przystąpili do regulacji internetu w sposób wycinkowy, każdy na własną rękę we własnym kraju. Przy czym już stosunkowo szybko uświadomiono sobie, że przestrzeń internetu nie może być i nie jest cyfrowym Dzikim Zachodem i dzisiaj co do zasady dominuje pogląd, że w przestrzeni wirtualnej obowiązują co do zasady te same normy, prawa i wymagania, które obowiązują w przestrzeni „realnej”. Pomimo to z każdym rokiem przybywa regulacji prawnych dedykowanych przestrzeni internetu, przy czym poszczególne kraje tworzą takie regulacje na własną rękę, w efekcie postępuje zjawisko tzw. fragmentaryzacji internetu, które w skrajnym scenariuszu doprowadzi do podziału globalnej sieci na regionalne i lokalne intranety nie komunikujące się swobodnie między sobą. Nikogo już dzisiaj nie trzeba przekonywać, że szeroko pojęty internet działa na innych zasadach i w innym otoczeniu prawnym w USA, w Europie, w Chinach i w innych częściach globu.

Bez względu na szlachetny cel, jakim jest ochrona małoletnich przed treściami pornograficznymi, projektowana ustawa jest kolejną cegiełką w postępującej fragmentaryzacji internetu.

Niemniej jednak negatywne skutki występują nie tylko w skali globalnej, a więc abstrakcyjnej i trudnej do przełożenia ma bieżące i lokalne potrzeby. Projektowana ustawa może być przysłowiową Puską Pandory polskiego internetu, inicjując trudny do zatrzymania proces, który może skończyć się tym, że w Polsce nie będzie już tzw. otwartego internetu, a zamiast tego będzie sieć oferująca dostęp do ograniczonego katalogu usług i treści, które przejdą przez szereg różnych filtrów, z których każdy będzie blokował inną kategorię treści i usług. Nie ulega wątpliwości, że treści pornograficzne to nie jest jedyne zagrożenie dla małoletnich w internecie. Jest wiele innych treści, usług i zjawisk, które mogą stanowić zagrożenie nie tylko dla dzieci, ale i dla dorosłych, jest wiele zachowań, zdarzeń, usług i treści, które są uznawane za szkodliwe albo niepożądane z tych czy innych względów.

Konstrukcja projektowanej ustawy może być przez przyszłych decydentów postrzegana jako doskonały instrument do wprowadzania obowiązku blokowania kolejnych i kolejnych kategorii treści, usług, zachowań i zdarzeń. Projektowana ustawa może w przyszłości stać się bazą, podstawą, do której legislacyjnie prostą nowelizacją będzie można dodawać kolejne kategorie blokowanych treści. A kolejka potencjalnych kandydatów na kolejne kategorie treści do blokowania jest bardzo długa i obejmuje treści terrorystyczne, przemoc, wulgaryzmy, hejt, narkotyki, alkohol, uzależnienia, piractwo, obraza uczuć religijnych, nieprawdziwe informacje, dezinformację i wiele, wiele innych.

## **VI. Prywatność abonentów**

Projektowana ustawa, w sposób zapewne niezamierzony, tworzy nowe zagrożenia dla prywatności abonentów i nie chodzi tu o przewidziany w projektowanej ustawie obowiązek raportowy wobec Ministra. Zakłada bowiem, że od decyzji abonenta zależało będzie, czy chce korzystać z blokowania treści pornograficznych, a więc siłą rzeczy u każdego dostawcy usługi dostępu do sieci internet powstaną dwie grupy abonentów, tych korzystających i tych nie korzystających z blokowania treści pornograficznych. Niestety projektowana ustawa zawiera przepisy, które będą zmuszały dostawców usługi dostępu do sieci internet do zbierania i przechowywania znacznie większej ilości informacji na temat korzystania (albo niekorzystania) z ustawowej blokady, niż jest to konieczne. Projektowana ustawa przewiduje bowiem, jako odrębny wymóg, obowiązek proponowania użytkownikowi końcowemu skorzystanie z blokady przed zawarciem umowy o świadczenie publicznie dostępnych usług telekomunikacyjnych oraz obowiązek udokumentowania faktu złożenia użytkownikowi końcowemu takiej propozycji (art. 3 ust. 2 projektowanej ustawy). W efekcie dostawcy internetu najprawdopodobniej będą zmuszeni od odbierania od użytkowników w jakiejś formie potwierdzenia, że użytkownikowi blokada została zaproponowana, celem wykonania obowiązku udokumentowania tego faktu. Ponadto, każdy użytkownik przed zawarciem umowy, po otrzymaniu propozycji korzystania z ustawowej blokady, będzie musiał zdecydować i swoją decyzję zakomunikować dostawcy internetu, czy chce czy nie chce z tej propozycji skorzystać. Ponadto, skoro prawem abonenta ma być możliwość złożenia, w dowolnym czasie żądania uruchomienia albo wyłączenia ustawowej blokady, a dostawca internetu będzie obowiązany te żądania zaspokoić w określonych w ustawie terminach, to dostawca usługi będzie zmuszony rejestrować choć podstawowe informacje pozwalające udowodnić (na potrzeby sporu z abonentem albo kontroli Ministra), że prawidłowo takie żądania obsłużył. W wykonaniu obowiązków wynikających z projektowanej ustawy dostawcy internetu będą musieli rejestrować zarówno własne działania jak i akty woli abonenta. Siłą rzeczy zatem projektowana ustawa tworzy po stronie dostawców internetu zbiór danych, który dla każdego indywidulanego abonenta będzie zawierał informację o tym, że abonentowi blokadę zaproponowano i o tym, czy abonent korzysta czy nie korzysta z ustawowej blokady.

Zmuszenie ustawą dostawców usługi dostępu do sieci internet do stworzenia i przechowywania takiego zbioru danych jest w sposób oczywisty zagrożeniem dla prywatności abonentów. Naturalnie dane abonentów i usługi, z których korzystają, są objęte ścisłą ochroną i przedsiębiorcy telekomunikacyjni

zrzeszeni w organizacjach sygnujących niniejsze stanowisko dokładają najwyższych starań organizacyjnych i technicznych, aby chronione dane nigdy nie wpadły w niepowołane ręce, ale trzeba pamiętać, że organy państwa oraz uprawnione podmioty mogą mieć dostęp do tego typu danych w świetle obowiązujących i projektowanych przepisów prawa. Organem kontrolującym wywiązywanie się przed dostawców internetu z obowiązków wynikających z projektowanej ustawy ma być minister właściwy do spraw informatyzacji, wspierany w tym przypadku przez Prezesa Urzędu Komunikacji Elektronicznej i to właśnie na potrzeby ministra właściwego do spraw informatyzacji i prowadzonych przez niego postępowań kontrolnych dostawcy internetu mają być zmuszeni do dokumentowania tak wielu czynności. Zatem dostęp do tych wszystkich danych i informacji będzie miał minister właściwy do spraw informatyzacji, a zapewne również Prezes UKE, w toku postępowań kontrolnych. Kwestią otwartą jest, czy dostęp do tych danych będą miały również tzw. uprawnione podmioty w rozumieniu art. 179 ust. 3 pkt 1) lit. a) ustawy – Prawo telekomunikacyjne, a więc Policja, Biuro Nadzoru Wewnętrzny, Straż Graniczna, Służba Ochrony Państwa, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Centralne Biuro Antykorupcyjne i Krajowa Administracja Skarbowa, realizujące swoje zadania na podstawie ustaw regulujących działalność tych służb oraz ustawy – Prawo telekomunikacyjne.

W dotychczasowej debacie nad tym zagadnieniem Projektodawca wielokrotnie podnosił, że zarzut zagrożenia dla prywatności dla abonentów jest niezasadny, gdyż raporty, które dostawcy internetu mają corocznie składać na ręce Ministra Cyfryzacji (art. 9 projektowanej ustawy) ma zawierać wyłącznie dane statystyczne, bez danych osobowych odnoszących się do indywidualnych abonentów. I faktycznie jako Izba nie widzimy zagrożenia dla prywatności abonentów w obowiązku raportowym, zagrożenie takie kryje się gdzie indziej i jak już wcześniej wyjaśniliśmy wynika z obowiązku dokumentowania faktu proponowania blokady i obowiązku obsługi żądań abonenta w terminach wynikających z projektowanej ustawy (art. 3 – 5), w połączeniu z uprawnieniami kontrolnymi Ministra Cyfryzacji (art. 11 i następne projektowanej ustawy).

## **ALTERNATYWA WOBEC MODELU ZAPROPONOWANEGO W PROJEKTOWANEJ USTAWIE**

Jak już wcześniej sygnalizowaliśmy rekomendowaną alternatywą wobec nowych ustawowych nakazów i zakazów jest zaangażowanie się instytucji i struktur Państwa Polskiego w działania edukacyjne i informacyjne, adresowane zarówno do rodziców i opiekunów, jak i dzieci, celem zwiększenia świadomości na temat zagrożeń jak również na temat sposobów i dostępnych już dzisiaj rozwiązań (w tym narzędzi technicznych) pomagających – każdemu chcącemu z nich korzystać – w chronieniu dzieci nie tylko przed dostępem do nieodpowiednich treści (rozumianych znacznie szerzej niż tylko treści pornograficzne), ale również pomagających w kontrolowaniu aktywności dzieci w świecie wirtualnym oraz kształtowaniu prawidłowych wzorców zachowań i postaw wobec uzależnień i innych zagrożeń związanych z elektroniką i światem cyfrowym. W ocenie Izby można zrobić znacznie więcej niż robione jest obecnie, aby zwiększyć odsetek rodziców i opiekunów korzystających z dostępnych już dzisiaj programów typu kontrola rodzicielska, a właśnie niskie wykorzystanie tego typu narzędzi jest – jak wynika z uzasadnienia do projektu ustawy – głównym powodem podjęcia przez Rząd interwencji legislacyjnej. Po drugie, zamiast na tworzeniu nowych regulacji prawnych sugerujemy skupienie uwagi Państwa Polskiego na egzekwowaniu już istniejących regulacji prawnych, których celem jest ochrona małoletnich przed dostępem do treści pornograficznych, takich jak art. 200 § 3 i 5 Kodeksu karnego.

Jeśli jednak w ocenie Projektodawcy nie może się obyć bez interwencji legislacyjnej, to zdecydowanie wskazujemy na rozwiązania wdrożone w Niemczech i we Francji oraz wdrażane w Wielkiej Brytanii, jako właściwy kierunek działania, który koresponduje również z funkcjonującymi w przestrzeni publicznej propozycjami organizacji społecznych zajmujących się ochroną małoletnich przed szkodliwym wpływem treści pornograficznych, takich jak Stowarzyszenie Twoja Sprawa. Zdecydowanie rekomendujemy kierunek i model opisany przez Projektodawcę w Ocenie Skutków Regulacji, a więc model który opiera się na następujących filarach i założeniach:

1. polskie prawo powinno nakazywać wszystkim (krajowym i zagranicznym) dostawcom treści pornograficznych stosowanie skutecznych mechanizmów weryfikacji wieku użytkownika (co jest naturalnym uzupełnieniem obowiązujących przepisów art. 200 § 3 i 5 Kodeksu karnego);
2. wybrany organ państwa (minister właściwy do spraw informatyzacji, Prezes UKE, NASK albo inny właściwy organ) powinien mieć kompetencję do badania, czy dostawca treści pornograficznych, udostępnianych lub rozpowszechnianych z wykorzystaniem środków komunikacji elektronicznej albo poprzez stronę internetową, wywiązuje się z obowiązku skutecznej weryfikacji wieku użytkownika; badanie takie powinno dotyczyć zarówno krajowych jak i zagranicznych dostawców treści pornograficznych; jeśli organ stwierdzi, że dostawca treści pornograficznych nie wywiązuje się z obowiązku skutecznej weryfikacji wieku, a treść udostępniana jest przez stronę internetową, to organ powinien móc podjąć decyzję o wpisaniu domeny takiej strony do rejestru blokowanych w Polsce domen internetowych; wybrany do tego zadania organ państwa powinien być wyposażony w niezbędne zasoby, powinien być również wspierany w swoich wysiłkach, w szczególności w zakresie identyfikowania serwisów nie stosujących skutecznych mechanizmów weryfikacji wieku, przez szeroko pojętą administrację publiczną, instytucje publiczne, organizacje społeczne, przedsiębiorców, rodziców, słowem każdego, kto może zauważyć i zgłosić do właściwego organu fakt istnienia strony internetowej oferującej dostęp do treści pornograficznych bez weryfikacji wieku;
3. przedsiębiorcy telekomunikacyjni świadczący usługę dostępu do sieci internet powinni być obowiązani do blokowania dostępu do domen wpisanych do rejestru, tj. zgodnie z wzorem istniejącego rejestru domen służących do oferowania gier hazardowych niezgodnie z ustawą (art. 15f ustawy o grach hazardowych).

Rozwijając wątek rejestru odradzamy tworzenie nowego rejestru blokowanych domen. Nie popieramy i nie rekomendujemy rozwiązań zmierzających do tworzenia kolejnych, „resortowych” rejestrów blokowanych domen. Na przestrzeni ostatnich kilku lat szereg ministerstw wystąpiło z projektami ustaw, które zakładały powoływanie kolejnych, „resortowych” rejestrów blokowanych domen internetowych. Konsekwentnie sprzeciwialiśmy się koncepcji rejestrów blokowanych domen, podkreślając jednocześnie, że jeżeli - pomimo zastrzeżeń przedsiębiorców telekomunikacyjnych - administracja publiczna zamierza wykorzystywać to narzędzie poprzez tworzenie kolejnych, „resortowych” rejestrów, to jedynym racjonalnym rozwiązaniem jest alternatywa w postaci stworzenia jednego, centralnie zarządzanego rejestru. Konsekwentnie pokazywaliśmy również problemy techniczne, prawne i ekonomiczne jakie wystąpią, jeśli Państwo Polskie doprowadzi do powstania więcej niż jednego, ustawowego rejestru blokowanych domen.

Rekomendowana koncepcja jednego rejestru zakłada, że w sensie technicznym będzie działał tylko jeden odpowiednio zorganizowany rejestr, który będzie mógł być zasilany wpisami różnych organów, którym ustawa przyzna kompetencję do dokonywania takich wpisów. Praktyczna realizacja tej koncepcji opiera się na wykorzystaniu istniejącego rejestru hazardowego, bez konieczności ingerencji w techniczną stronę funkcjonowania rejestru, z integracją na poziomie legislacyjnym. Szczegóły tej koncepcji były prezentowane w toku prac legislacyjnych nad projektami kolejnych ustaw zakładających stworzenie „resortowych” rejestrów. Przykładowo, takie stanowiska Izba przedstawiła wobec projektu ustawy *o zmianie ustawy o ochronie konkurencji i konsumentów* (UC15), procedowanego przez Prezesa UOKiK: <https://legislacja.rcl.gov.pl/docs//2/12338717/12724859/12724862/dokument497135.pdf>), w którym pierwotnie zakładano powołanie nowego, zarządzanego przez Prezesa UOKiK rejestru blokowanych domen (niezależnego od rejestru hazardowego). W toku konsultacji publicznych projektu ustawy UC15 UOKiK uwzględnił postulaty i propozycje zgłoszone w zakresie dotyczącym rejestru, a najnowsza wersja projektu ustawy rezygnuje z tworzenia nowego rejestru, zamiast tego dając Prezesowi UOKiK kompetencję do występowania do Ministra Finansów z wnioskiem o wpisanie wskazanej przez Prezesa UOKiK domeny do istniejącego rejestru hazardowego, zarządzanego przez Ministra Finansów. Rekomendujemy zatem, na wzór rozwiązania przyjętego przez UOKiK w najnowszej wersji projektu ustawy

UC15, wyposażenie właściwego organu (ministra właściwego do spraw informatyzacji, Prezesa UKE, NASK albo innego właściwego organu) w ustawową kompetencję do występowania do Ministra Finansów z wnioskiem o wpisanie domeny wykorzystywanej do udostępniania treści pornograficznych bez skutecznego mechanizmu weryfikacji wieku do istniejącego rejestru hazardowego, działającego na podstawie art. 15f ustawy o grach hazardowych. Tak wpisana domena zostanie zablokowana przez dostawców internetu w wykonaniu obowiązku wynikającego z art. 15f ust. 5 ustawy o grach hazardowych, bez konieczności regulowania procesu blokowania w przepisach projektowanej ustawy. Koncepcja ta wymaga wprowadzenia do projektowanej ustawy (na wzór projektu ustawy UC15) przepisu dającego wybranemu organowi kompetencję do występowania do Ministra Finansów o wpisanie do rejestru hazardowego domen oferujących treści pornograficzne bez wymaganej, skutecznej weryfikacji wieku.

W tym miejscu zwracamy uwagę, że proponowany model alternatywny (wzorowany na rozwiązaniach francuskich i niemieckich) jest znacznie lepszy od modelu zaproponowanego w projektowanej ustawie, gdyż jest pozbawiony większości jego wad, a mianowicie:

1. model alternatywny nie jest niezgodny z prawem UE, gdyż nie nakłada na przedsiębiorcę telekomunikacyjnego ogólnego obowiązku monitorowania treści dostępnych w internecie;
2. model alternatywny stanowi logiczne rozwinięcie i uzupełnienie obowiązujących przepisów prawa (Kodeks karny), a jego wdrożenie w zakresie dotyczącym blokowania domen nie wymaga prowadzenia żadnych prac wdrożeniowych i żadnych nakładów publicznych w tym zakresie, gdyż każda domena wpisana do rejestru hazardowego będzie blokowana przez dostawców internetu na zasadach określonych w ustawie o grach hazardowych;
3. model alternatywny nie wyklucza i nie deprecjonuje znaczenia wychowania, edukacji i informacji, nie tworzy złudnego przeświadczenia o „załatwieniu sprawy”, nie sugeruje, że nie trzeba robić nic więcej, pozostawiając przestrzeń dla działań edukacyjnych i informacyjnych celem zwiększenia poziomu wykorzystania istniejących rozwiązań technicznych; ponadto, model alternatywny pozostawia przestrzeń do dalszego rozwoju i doskonalenia palety dobrowolnych rozwiązań technicznych;
4. model alternatywny jest bez wątpienia bardziej sprawiedliwy niż model zaprezentowany w projektowanej ustawie, gdyż zdecydowanie lepiej identyfikuje role i odpowiedzialność za treści pornograficzne przypisuje dostawcom tych treści, a nie dostawcom łączności; jednocześnie model ten przewiduje rolę dla organów Państwa Polskiego, które powinno być zaangażowane w ochronę dzieci przed szkodliwym wpływem treści pornograficznych;
5. model alternatywny nie tworzy poważnych zagrożeń dla prywatności użytkowników internetu z perspektywy informacji gromadzonych przez dostawcę internetu w wykonaniu przepisów, gdyż zakłada, że dostęp do domeny umieszczonej w rejestrze byłby blokowany każdemu abonentowi (z mocy ustawy), a więc nie powstawałyby bazy abonentów chcących i nie chcących mieć dostępu do treści pornograficznych (jak w przypadku modelu zaproponowanego w projektowanej ustawie);
6. model alternatywny nie będzie mógł być tak łatwo wykorzystany do obejmowania nim kolejnych kategorii treści, gdyż wymaga zaangażowania organów państwa i stworzenia po stronie administracji publicznej odpowiednich zasobów kadrowych i kompetencyjnych, co będzie stanowiło naturalne ograniczenie przed pochopnym dodawaniem kolejnych kategorii treści lub usług do zakresu przedmiotowego takiej ustawy;
7. model alternatywny nie wymaga „wymyślenia koła na nowo”, wzoruje się na mechanizmach francuskich, niemieckich i brytyjskich, a więc pozwala na budowanie na doświadczeniach zebranych przez europejskich partnerów.

Podsumowując, jeśli w ocenie Projektodawcy interwencja legislacyjna jest konieczna, to zdecydowanie rekomendujemy zaprojektowanie ustawy na wzór mechanizmów wdrożonych we Francji i w Niemczech,



wdrażanych w Wielkiej Brytanii i funkcjonujących już jako propozycje w krajowym dyskursie publicznym za sprawą Stowarzyszenia Twoja Sprawa.

Niniejsze stanowisko jest również dobrym miejscem do odniesienia się do argumentacji, którą posługiwał się Projektodawca na etapie konsultacji publicznych projektowanej ustawy, dla uzasadnienia decyzji o odrzuceniu proponowanego przez Izbę i stosowanego w Europie Zachodniej rozwiązania alternatywnego dla modelu przedstawionego w projektowanej ustawie. W tabeli z konsultacji publicznych może przeczytać, że Projektodawca odrzucił rozwiązanie oparte o rejestr publiczny z powodów, które można podzielić na dwie podstawowe grupy:

- a. obawy Projektodawcy o to, że stworzenie publicznego rejestru blokowanych stron pornograficznych byłoby kontr-produktywne, zwiększając zamiast zmniejszając wśród małoletnich świadomość na temat dostępnych w internecie treści pornograficznych;
- b. obawy Projektodawcy o to, że nałożenie na dostawców treści pornograficznych obowiązku weryfikacji wieku użytkownika stanowiłoby zagrożenie dla bezpieczeństwa danych osobowych i prywatności użytkowników.

W ocenie Izby żaden z powyższych argumentów nie jest trafiony. Jeśli chodzi o publiczny rejestr domen do blokowania, to choć dostawcy internetu co do zasady nie popierają tworzenia takich rejestrów (w szczególności rejestrów rozproszonych), to w zestawieniu z obowiązkiem identyfikowania i blokowania wszystkich stron internetowych zawierających treści pornograficzne (nawet na żądanie abonenta), rejestr wydaje się rozwiązaniem bardziej racjonalnym. A jednocześnie zdziwienie budzi argumentacja Projektodawcy, z której ma wynikać, że istnienie rejestru blokowanych domen w zasadzie zachęca do ich odwiedzania albo w inny sposób przyczynia się do zwiększenia zainteresowania zawartością blokowanych domen. Gdyby tak było, to trzeba by dojść do dosyć absurdalnych wniosków, że prowadzony na podstawie ustawy o grach hazardowych przez Ministra Finansów rejestr domen służących do oferowania gier hazardowych niezgodnie z ustawą w rzeczywistości stanowi zachętę do korzystania z nielegalnego hazardu on-line. Zgodnie z logiką zaproponowaną przez Projektodawcę w tabeli z konsultacji publicznych, istniejącą z inicjatywy Ministra Cyfryzacji i Prezesa UKE listę ostrzeżeń przed niebezpiecznymi stronami, prowadzoną przez CSIRT NASK<sup>8</sup>, należałoby uznać za zachętę do ryzykownych zachowań, a nie wprowadzone w związku z COVID-19 narzędzie chroniące miliony obywateli przed utratą pieniędzy i kradzieżą tożsamości. Argumentacja wykorzystana przez Projektodawcę do odrzucenia możliwości stworzenia rejestru domen jest w sposób oczywisty nie do przyjęcia, a Państwo jako całość nie może traktować tego samego narzędzia (rejestru) jako środek ograniczający i jednocześnie wzmacniający określone, negatywne zjawisko społeczne.

Argumentacja Projektodawcy dotycząca obaw o prywatność użytkowników, którzy musieliby podawać swoje dane osobowe dostawcom treści pornograficznych na potrzeby weryfikacji wieku, bez wątplenia płynie z realnej troski Projektodawcy o prywatność obywateli. Niemniej jednak ta argumentacja nie uwzględnia roli postępu, jak również otaczającej nas rzeczywistości i obowiązujących już w Polsce przepisów prawa.

W pierwszej kolejności należy zwrócić uwagę, że znane są opracowania koncepcyjne pozwalające na skuteczną weryfikację wieku on-line bez konieczności udostępniania dostawcy treści pornograficznych danych osobowych użytkownika. Bez wątplenia wdrożenia takich mechanizmów stanowiłoby wyzwanie, ale jest to wyzwanie warte podjęcia w imię tworzenia skutecznego i sprawiedliwego prawa. Po wtóre, argumentacja Projektodawcy wydaje się pomijać fakt, że już dzisiaj wielu pełnoletnich użytkowników, poszukujących dostępu do treści pornograficznych (które jako takie nie są nielegalne), jest gotowych nie tylko udostępnić dostawcy takich treści swoje dane osobowe (np. na potrzeby założenia konta w serwisie) ale jest gotowych płacić za takie treści, nierzadko przekazując dostawcy treści pornograficznych numery kart płatniczych. Bez względu na to, jak oceniane może być takie zachowanie, faktem pozostaje, że jeśli

---

<sup>8</sup> [https://cert.pl/posts/2020/03/ostrezenia\\_phishing/](https://cert.pl/posts/2020/03/ostrezenia_phishing/)

dostęp do treści pornograficznych uzyskuje osoba pełnoletnia to taka osoba musi samodzielnie ocenić, czy chce i jest gotowa zaakceptować ryzyka związane z udostępnieniem swoich danych osobowych i płatniczych dostawcy treści pornograficznych. Wreszcie argumentacja Projektodawcy pomija całkowicie obowiązujące już w Polsce przepisy prawa. Jako Izba już w październiku 2022 r., w stanowisku złożonym w ramach konsultacji publicznych, podnosiliśmy, że projektowana ustawa powinna budować na obowiązujących w Polsce przepisach prawa, a publiczny rejestr domen wydaje się naturalnym rozwinięciem obowiązujących przepisów. Ponownie przypominamy, że zgodnie z art. 200 ust. 3 i 5 Kodeksu karnego:

*§ 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.*

*§ 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.*

Zatem już dzisiaj w Polsce przestępstwem jest m.in. rozpowszechnianie treści pornograficzne w sposób umożliwiający małoletniemu zapoznanie się z nimi oraz prowadzenie reklamy lub promocji działalności polegającej na rozpowszechnianiu treści pornograficznych w sposób umożliwiający zapoznanie się z nimi małoletniemu. Każdy kto rozpowszechnia treści pornograficzne w internecie, jeśli nie chce popełnić przestępstwa, powinien zapewnić, że małoletni nie uzyska dostępu do tak rozpowszechnianych treści. A to oznacza, że każdy kto rozpowszechnia treści pornograficzne w internecie już dzisiaj musi – jeśli nie chce popełnić przestępstwa – weryfikować wiek użytkownika żądającego dostępu do treści, tak, aby tego dostępu nie dać małoletniemu. Zatem już dzisiaj obowiązujące w Polsce przepisy prawa wymagają od dostawców treści pornograficznych weryfikacji wieku użytkownika. Niestety przepis ten wydaje się pozostawać w dużej mierze martwy, ale raczej nie ze względu na obawy o to, że rozpoczęcie jego egzekwowania zagrazi prywatności obywateli, a ze względu na niemoc egzekucyjną Państwa, które w tej sytuacji woli tworzyć kolejne przepisy i obowiązki, zamiast zastanowić się nad poprawą egzekwowalności istniejących przepisów. W ocenie Izby rozwiązania niemieckie, francuskie i wdrażane w Wielkiej Brytanii są narzędziami pozwalającymi na skuteczne egzekwowanie przepisów takich jak polski art. 200 Kodeksu karnego, gdyż wprowadzają narzędzie (blokady dostępu do wpisanej do rejestru domeny internetowej, której właściciel nie stosuje skutecznych mechanizmów weryfikacji wieku), pozwalające na egzekwowanie takich przepisów również w przypadku, gdy dostawca treści pornograficznych znajduje się za granicą.

## **TERMIN WEJŚCIA W ŻYCIE PROJEKTOWANEJ USTAWY**

Projekt ustawy przewiduje, że dostawcy internetu, nie będący mikro przedsiębiorcami, małymi przedsiębiorcami albo średnimi przedsiębiorcami, będą zmuszeni do wywiązywania się z obowiązków przewidzianych w projektowanej ustawie począwszy od dnia 1 września 2023 r. tak określony termin jest terminem nierealnym i jako taki powinien być zmieniony, na taki, który bardziej niż kalendarzem politycznym będzie kierował się tym co technicznie wykonalne, racjonalne i dopuszczalne w demokratycznym państwie prawa.

Już w ramach konsultacji publicznych podnosiliśmy, że Projektodawca przyjął dalece upraszczające założenia, że każdy duży przedsiębiorca telekomunikacyjny już dzisiaj oferuje rozwiązania techniczne do ochrony dzieci w świecie cyfrowym i na podstawie tego założenia przyjął kolejne założenie, że w przypadku tej kategorii przedsiębiorców telekomunikacyjnych przejście od obecnie oferowanych rozwiązań do ustawowego obowiązku blokowania treści pornograficznych będzie łatwym i szybkim procesem. Zwracaliśmy uwagę, że oferowane obecnie, zarówno płatne jak i bezpłatne rozwiązania, różnią się istotnie od tego, co będzie wymagane na gruncie projektowanej ustawy. Obecnie oferowane usługi, czy to

sieciowe, czy aplikacyjne, najczęściej stanowią zintegrowaną usługę na którą składa się kontrola rodzicielska obejmująca znacznie szerszy zakres funkcjonalności i blokad niż tylko treści pornograficzne, uzupełniana programami antywirusowymi. Kształt tych rozwiązań, jak również model, w którym są oferowane (odpłatne, bezpłatne) zależy do umów pomiędzy dostawcą internetu a zewnętrznym partnerem, który dostarcza niezbędną technologię. Nieuzasadnione jest założenie, że da się w prosty sposób wyodrębnić z istniejącej oferty blokadę treści pornograficznych i uczynić z niej blokadę ustawową, przy jednoczesnym zachowaniu pozostałych warunków współpracy z zewnętrznymi dostawcami bez zmian. Już teraz jasnym jest, że istniejące modele współpracy i istniejące rozwiązania techniczne będą musiały zostać poważnie zmienione pod wpływem projektowanej ustawy, w niektórych przypadkach wymuszając wręcz rezygnację z obecnie oferowanych rozwiązań i stworzenie w ich miejsce nowych, uwzględniających nowe otoczenie regulacyjne. Ponadto, nie sposób nie zauważyć, że dostosowanie się do wymagań wynikających z projektowanej ustawy to nie tylko kwestia opracowania we własnym zakresie albo zakupu od dostawcy zewnętrznego określonego rozwiązania technicznego (sieciowego lub aplikacyjnego) ale również zmian w dokumentach, procesach obsługi klienta oraz systemach dostawcy usługi dostępu do sieci internet, wynikających z szeregu nowych obowiązków dokumentacyjnych, obsługowych, informacyjnych i raportowych zapisanych w projektowanej ustawie, towarzyszących obowiązkowi głównemu, polegającemu na blokowaniu stron na żądanie abonenta. Dodatkowe wyzwania pojawią się tam, gdzie detaliczny dostawca internetu świadczy usługi z wykorzystaniem sieci partnera hurtowego, jak to ma miejsce w przypadku operatorów MVNO czy współpracy hurtowej na rynku stacjonarnym. W zależności od biznesowego modelu i technologicznej platformy współpracy wywiązanie się z obowiązku blokowania treści pornograficznych przez dostawców detalicznych może wymagać czasochłonnych i kosztownych prac wdrożeniowych we współpracy z partnerami hurtowymi.

Wyznaczenie 1 września 2023 r. jako termin wejścia w życie przepisów oznacza, że Projektodawca nie tylko zignorował nasze słuszne postulaty i argumenty, ale wręcz zamierza – z podeptaniem zasad demokratycznego państwa prawa - pozbawić większych dostawców internetu jakiegokolwiek czasu na przygotowanie się i wdrożenie wymagań wynikających z projektowanej ustawy. Biorąc pod uwagę kalendarz legislacyjny trudno zakładać, że ustawa zostanie przyjęta przez Sejm i Senat wcześniej niż latem tego roku. Zatem jeśli ustawa ma wejść w życie 1 września 2023 r. to wysoce prawdopodobne jest, że pomiędzy publikacją ustawy w Dzienniku Ustaw a wejściem w życie obowiązków nie będzie potrzebnego i rozsądnego odstępu czasu pozwalającego dostawcom internetu na przygotowanie się i wdrożenie nowych obowiązków. Demokratyczne państwo prawa nie może wymagać od swoich obywateli i przedsiębiorców, aby dostosowywali się do nowych wymagań i obowiązków nie na podstawie ogłoszonego w Dzienniku Ustaw prawa, a na podstawie projektów aktów prawnych, które zmieniają się w toku prac legislacyjnych. W demokratycznym państwie prawa właśnie po to jest *vacatio legis*, aby adresaci (obywatele, przedsiębiorcy) nowych obowiązków mogli się do nich dostosować wiedząc już jak finalnie brzmi nowy obowiązek, ogłoszony w Dzienniku Ustaw, a okres ten powinien być adekwatny do skali niezbędnych przygotowań, nakładów i wysiłku potrzebnego do przygotowania się do nowego obowiązku. 1 września 2023 r. jest terminem nierealistycznym, a już na pewno niezwykle trudnym dla dostawców internetu, gdyż nie uwzględnia skali wyzwania i problemów, z jakimi będą musieli zmierzyć się przedsiębiorcy telekomunikacyjni, aby wywiązać się z nowych obowiązków. W tym przypadku za racjonalne minimum uznajemy *vacatio legis* wynoszące 6 miesięcy liczone od dnia ogłoszenia ustawy w Dzienniku Ustaw.

Jeśli celem faktycznie jest ochrona małoletnich, a nie kampania wyborcza, nie powinno być przeciwskażeń do przyjęcia takiego terminu wejścia w życie projektowanych przepisów, aby dostawcy internetu mieli niezbędną ilość czasu na przygotowanie się do realizowania nowych obowiązków i wdrożenie mechanizmów efektywnie chroniących dzieci przed kontaktem z treściami pornograficznymi, nawet jeśli oznacza to, że narzędzia te zaczną funkcjonować już po wyborach, na gruncie ustawy przyjętej przed wyborami.

W związku z powyższym prosimy o taką zmianę projektowanej ustawy, aby wszystkie obowiązki adresowane na dostawców usługi dostępu do sieci internet, związane z ograniczaniem małoletnim dostępem do treści pornograficznych w internecie, wchodziły w życie po upływie 6 miesięcy od dnia ogłoszenia ustawy w Dzienniku Ustaw.

Ponadto, zwracamy uwagę, że nierealistycznie określony termin wejścia w życie projektowanej ustawy może być problemem nie tylko dla większych dostawców internetu, ale również dla mniejszych dostawców internetu jak i dla podmiotów oferujących Wi-Fi jako element dodatkowy wobec podstawowej działalności (restauracje, hotele, sklepy, punkty usługowe itd.). W efekcie uwag owych „mniejszych” podmiotów formułowanych na etapie konsultacji publicznych Projektodawca komunikował, że owe „mniejsze” podmioty będą miały 24 miesiące na dostosowanie się. Niestety deklaracje te nie do końca znajdują potwierdzenie w tekście przedłożenia rządowego. Zwracamy bowiem uwagę, że przepis określający termin wejścia w życie obowiązków sformułowany jest w następujący sposób:

*Art. 41. Ustawa wchodzi w życie z dniem 1 września 2023 r., z wyjątkiem:*

*1) art. 11–21 oraz art. 23–25 w zakresie dostawców usługi dostępu do sieci internet będących w dniu wejścia w życie ustawy mikroprzedsiębiorcami, małymi przedsiębiorcami i średnimi przedsiębiorcami, o których mowa odpowiednio w art. 7 ust. 1 pkt 1–3 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców, które wchodzi w życie po upływie 24 miesięcy od dnia ogłoszenia;*

*2) art. 11–15 oraz art. 22 w zakresie przedsiębiorców, o których mowa w art. 10 ust. 1, które wchodzi w życie po upływie 24 miesięcy od dnia ogłoszenia;*

*[...]*

Jak więc widać zarówno mali dostawcy internetu (punkt 1) jak i dostawcy Wi-Fi (punkt 2) będą mieli już od 1 września 2023 r. prawny obowiązek proponowania i świadczenia na żądanie abonenta usługi blokowania stron internetowych zawierających treści pornograficzne, obowiązek udostępniania odpowiednich informacji na stronie, obowiązek posiadania regulaminu usługi, obowiązek raportowy wobec Ministra i obowiązek oferowania Wi-Fi bez treści pornograficznych, skoro obowiązki te wynikają z art. 3 – 10 projektowanej ustawy, a te artykuły jak widać powyżej nie są objęte 24 miesięczną derogacją. Owe 24 miesiące dotyczy bowiem tylko tych przepisów ustawy, które dają Ministrowi Cyfryzacji uprawnienia do prowadzenia kontroli i nakładania kar za niewywiązanie się z obowiązków ustawowych. Czy zatem analizowane przepisy należy czytać w ten sposób, że również mali dostawcy internetu i dostawcy Wi-Fi będą prawnie zobowiązani wykonywać obowiązki wynikające z projektowanej ustawy już w terminie 1 września 2023 r., ale Minister Cyfryzacji nie będzie miał przez 24 miesiące prawa do kontrowania i karania tych podmiotów? Jeśli tak, to konstrukcja taka odbiega od deklaracji składanych w tym zakresie przez Rząd i nawet jeśli chroni przez jakiś czas małych dostawców internetu i dostawców Wi-Fi przed kontrolami karami, to przecież nie chroni przed roszczeniami abonentów, którzy już od 1 września 2023 r. będą mogli domagać się od tych podmiotów realizacji swoich uprawnień wynikających z ustawy. Jeśli zapis jest wynikiem błędu legislacyjnego to wymaga poprawy, jeśli jest zabiegiem celowym to w ocenie Izby koncepcja ta wymaga weryfikacji, gdyż wydaje się wysoce niedoskonała i problematyczna.