GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Wojciech R. Wiewiórowski

GI-035-6|13|58878

Warszawa, dnia 11 września 2013 r.

Pani
Julia Pitera
Przewodnicząca Komisji
Administracji i Cyfryzacji
Sejm Rzeczypospolitej Polskiej
ul. Wiejska 4 / 6 /8
00 – 902 Warszawa

Szanowna Pani Przewodnicząca

W związku przedstawionym przez posłów **projektem uchwały Sejmu Rzeczypospolitej Polskiej wzywającej Ministra Administracji i Cyfryzacji do zagwarantowania rodzicom prawa do Internetu bez pornografii** (Druk Sejmowy nr 1664) pragnę przedstawić Wysokiej Komisji stanowisko polskiego organu ochrony danych osobowych dotyczące prawnej regulacji utrudniania dostępu do stron i usług internetowych poprzez filtrowanie komunikacji pomiędzy użytkownikiem Internetu, dostarczycielem usług internetowych i dostarczycielem treści.

Tematyka ta pozostaje w obszarze zainteresowania Generalnego Inspektora Ochrony Danych Osobowych. Dokonywanie jakiegokolwiek filtrowania komunikacji pomiędzy uczestnikami obrotu internetowego może prowadzić – i w wielu sytuacjach prowadzi – do przetwarzania dodatkowych danych osobowych dotyczących użytkowników sieci. Może również ingerować w treść komunikatu. Oznacza to, że działania takie będą prowadziły do ograniczenia konstytucyjnie gwarantowanych prawa do prywatności (art. 47 Konstytucji RP), prawa do ochrony danych osobowych (art. 51 Konstytucji RP) oraz wolności komunikacji (art. 49 Konstytucji RP). Ingerencja taka, jeśli uznana byłaby za wskazaną, mogłaby nastąpić tylko z poszanowaniem testu niezbędności w demokratycznym państwie prawnym, o którym mowa w art. 31 Konstytucji RP.

ul. Stawki 2
00 – 193 Warszawa
tel.(022) 860 – 70 – 81
fax (022) 860 – 70 – 90
www.giodo.gov.pl

1. **Zgadzając się posłami zgłaszającymi projekt uchwały co do diagnozy postawionej w sprawie rozszerzającej się dostępności dla dzieci treści pornograficznych w sieci, muszę jednak podkreślić, że proponowane rozwiązanie tego problemu wydaje się błędne, nieskuteczne i grozić może bardzo niekorzystnymi zmianami w sposobach gromadzenia informacji o osobach fizycznych.** Zdaniem Generalnego Inspektora Ochrony Danych Osobowych wykazanie niezbędności tego typu ingerencji będzie bardzo trudne, o czym świadczyć może również dyskusja prowadzona w latach 2009-2010 nad tzw. Rejestrem Stron i Usług Niedozwolonych. Rozwiązanie to promowane wówczas przez Radę Ministrów spotkało się z dużymi wątpliwościami, które ostatecznie doprowadziły do zarzucenia tej idei i oświadczenia ze strony Prezesa Rady Ministrów, że powrót do dyskusji nad prawnymi rozwiązaniami dotyczącymi tej sfery może nastąpić tylko po dogłębnych konsultacjach społecznych.

Niniejszym pozwalam sobie zgłosić chęć udziału w tych konsultacjach, zwracając jednocześnie uwagę na szereg technicznych problemów, które były już dyskutowane przy tworzeniu tzw. Rejestru Stron i Usług Niedozwolonych i zostały podsumowane w rekomendacji Zespołu Zadaniowego Komitetu Rady Ministrów ds. Informatyzacji i Łączności w sprawie zmian do ustawy prawo telekomunikacyjne zamieszczonych w projekcie ustawy o zmianie ustawy o grach hazardowych oraz niektórych innych ustaw z grudnia 2009 r.

2. Utrudnianie dostępu do treści zawierających materiały pornograficzne jest już dziś stosowane w niektórych państwach świata, wśród nich również w takich państwach, które powszechnie uznajemy za demokratyczne (np. Australia, Dania, Finlandia, Niemcy, Norwegia, Szwecja, Włochy, Wielka Brytania). Przed podjęciem ewentualnej dyskusji o wprowadzeniu podobnych rozwiązań w Polsce niezbędne wydaje się przeanalizowanie skuteczności rozwiązań przyjętych w tych krajach oraz adekwatności środków wydanych tak przez instytucje publiczne jak przez przedsiębiorców na spełnienie wymagań prawnych w stosunku do celu, który ma zostać osiągnięty. Nie negując, że problem dostępności pornografii dziecięcej i innych rodzajów pornografii zabronionych rzez prawo polskie jest problemem o charakterze społecznym, rzeczywista skuteczność filtrowania sieci lub blokowania dostępu do konkretnych zasobów jest zazwyczaj kwestionowana. Pojawiają się wręcz ironiczne stwierdzenia – choćby po zapowiedzi Premiera Wielkiej Brytania dotyczącej rozszerzenia filtrowania sieci w jego kraju – że odcinanie młodym ludziom dostępu do treści internetowych jest „doskonałym sposobem na promowanie umiejętności hakerskich wśród dzieci i młodzieży". Trzeba również zwrócić uwagę na to, że nieskuteczny system filtrowania sieci powoduje fałszywe poczucie rozwiązania problemu społecznego w sytuacji gdy problemem jest nie dostęp do informacji sprzecznej z prawem, lecz samo dystrybuowanie tej informacji.

Trzeba pamiętać, że jakakolwiek działalność polegająca na filtrowaniu informacji i blokowaniu dostępu do niej, która w oczywisty sposób będzie połączona również z wprowadzeniem sankcji za nieprzestrzeganie odpowiednich przepisów bywa traktowana jako substytut dla istniejących już w dzisiejszym prawie środków przeciwdziałania dostępności treści niezgodnych z prawem poprzez stosowanie urzędowych wezwań, o których mowa w art. 14 ustawy o świadczeniu usług drogą elektroniczną i w odpowiadającym mu art. 14 Dyrektywy 2000/31/WE Parlamentu i Rady WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku.

3. Przechodząc do oceny propozycji zawartych w projekcie uchwały i jej uzasadnieniu należy zwrócić uwagę na początku na to, że **choć zdaniem projektodawców uchwała proponuje rozwiązanie bardziej przyjazne niż proponowane przez premiera Wielkiej Brytanii Davida Camerona, to w praktyce proponowane rozwiązanie jest jeszcze bardziej niebezpieczne dla prywatności osób niż propozycja brytyjska**. Brytyjski premier chce, by deklarowano ewentualną chęć dostępu do treści pornograficznych, zaś wnioskodawcy proponują, aby każdy użytkownik Internetu mógł zażądać od swojego dostawcy usług internetowych zablokowania dostępu do treści pornograficznych. W zamiarze projektodawców każda osoba powinna mieć prawo żądania od dostawcy usług internetowych blokowania przesyłania treści o charakterze pornograficznym, zaś dostawca usług internetowych jest zobowiązany do zapewnienia prawa do Internetu bez pornografii nieodpłatnie.

Należy zacząć od wyjaśnienia **niepewności co do pojęcia "dostawcy usług internetowych"**. W dalszej części opinii przyjmuję, że chodzi tu o "dostarczyciela dostępu do Internetu" (*Internet Access Provider*), gdyż stosowanie takiego pojęcia wobec dostarczycieli treści (*Internet Content Providers*) prowadziłoby do rozwiązań absurdalnych. Nawet jednak przy takim ograniczeniu nie wiadomo jak daleko się gać powinna ta definicja, a w szczególności czy dotyczy ona podmiotów umożliwiających dostęp do sieci Wi-Fi (i podobnych rozwiązań). Jeśli bowiem przyjąć, że każdy z nas będzie mieć prawo żądania od dostawcy usług internetowych blokowania przesyłania treści o charakterze pornograficznym, to o ile z zasady mamy praktyczną możliwość ustalenia z jakiej sieci Wi-Fi korzystamy, o tyle oczywiście nie wiemy od kogo mielibyśmy żądać realizacji prawa, jeśli taki obowiązek odnosiłby się do dostarczyciela dostępu do sieci publicznej. Zasiadając na przykład w sali obrad Komisji Sejmowej, niektórzy z nas korzystają z otwartej sieci Wi-Fi Kancelarii Sejmu przeznaczonej dla prasy. Jeśli zbliżymy się do budynku Senatu - z sieci Kancelarii Senatu. Te dwa podmioty będą zatem "dostarczycielami dostępu do Internetu", od których powinniśmy żądać zrealizowania naszego prawa. Podobny wniosek - bo zapewne odbywałoby się to w trybie wnioskowym - skierować zapewne powinienem do dostarczyciela

sygnału telewizji kablowej, z którego usług korzystam w domu, do przedsiębiorcy telekomunikacyjnego, który "dostarcza mi Internetu" przy pomocy przenośnego urządzenia USB oraz do Biura GIODO. **Każdy z tych podmiotów stałby się administratorem "bazy sprzeciwów" zgłoszonych przez osoby fizyczne, która była by sama w sobie zbiorem danych osobowych, podlegającym wszystkim obowiązkom wynikającym z ustawy o ochronie danych osobowych.** Oczywiście **alternatywą jest stworzenie centralnego rejestru takich sprzeciwów,** ale powstają wówczas pytania o to, kto powinien go prowadzić, jak powinien "rozprzestrzeniać" informację o sprzeciwie i - oczywiście - z jakich środków publicznych sfinansować stworzenie u utrzymanie takiej infrastruktury ? Wyjaśnienie, że takie działanie jest - jak wymagają tego art. art. 31 i 51 Konstytucji RP - jest niezbędne w demokratycznym państwie prawnym będzie zaś praktycznie niemożliwe.

4. W tych rozważaniach nie można też pominąć innego problemu. **Konstrukcja proponowanego uprawnienia jako uprawnienia podmiotowego nie może sprawdzić się w sytuacji, gdy nie ma** - i oby nie było - **obowiązku identyfikowania się przy dostępie do sieci.** Takie uprawnienie może być zrealizowane tylko poprzez filtrowanie dostępu do danych z konkretnego urządzenia. Nawet jeśli technicznie takie rozwiązanie mogłoby być w przyszłości możliwe - szczególnie po upowszechnieniu się protokołu IPv6 - to trudno wyobrazić sobie, by w takich "rejestrach sprzeciwów" znalazły się numery IP (v6) przywiązane na stałe do wszystkich urządzeń, z których rodzice i/lub dzieci korzystają. Pomijamy problem istnienia różnych profili użytkownika na jednym urządzeniu.

5. Kolejnym problemem w taki systemie jest **nadmierne zbieranie danych o zachowaniach osoby w sieci.** Ponieważ dostawca usług internetowych zdaniem projektodawców powinien być odpowiedzialny za opracowanie skutecznych filtrów, które umożliwią blokowanie przesyłania treści o charakterze pornograficznym, należy domniemywać, że po pierwsze każdy z wymienionych podmiotów (z Kancelarią Sejmu włącznie) byłby **odpowiedzialny za ustalenie co jest pornografią, a co nie jest.**

Po drugie zaś - ponieważ podlega odpowiedzialności (zapewne - co byłoby logiczne - również karnej) - **ma uzasadniony interes w gromadzeniu pełnej informacji o naszej działalności w sieci,** by w razie dochodzenia od niego odpowiedzialności za nieprawidłowo wykonaną przymusową usługę, móc poprawnie przeprowadzić procedurę "reklamacyjną". Będzie więc zmuszony przechowywać historię połączeń użytkownika z konkretnymi stronami w sieci. W tej sytuacji bardzo niepokojące mogą być uprawnienia policji i innych służb publicznych dostępu do takich danych na podstawie art. 18 ustawy o świadczeniu usług drogą elektroniczną.

Kolejne uwagi odnoszą się do wszelkich metod filtrowania niezależnie od tego, czy blokowany byłby cały ruch, czy tylko ruch do wybranych użytkowników, którzy skorzystali ze swego prawa podmiotowego, które statuują projektodawcy.

6. Prowadzone wcześniej w Polsce dyskusje na temat utrudniania dostępu do informacji w sieci bardzo szybko wykraczały poza powszechnie akceptowany problem prawnie regulowanej niedozwolonej pornografii i praktycznie natychmiast dotyczyły również blokowania dostępu do treści, np. związanych z hazardem elektronicznym, propagandą faszystowską lub inną totalitarną, czy w końcu zwalczania oszustw w sieci. Trzeba domniemywać, że **ewentualne wprowadzenie do polskiego porządku prawnego przepisów dotyczących utrudniania dostępu do informacji w sieci natychmiast będzie rozszerzone poza dyskutowane dziś ramy niedozwolonych rodzajów pornografii.**

7. Podstawowym utrudnieniem przy prowadzeniu jakiejkolwiek dyskusji na temat skuteczności takich działań jest – na co wskazywano już w 2009 r. – **brak możliwości określenia parametrów statystycznych skuteczności blokowania stron internetowych i usług**. Taka statystyka mogłaby zostać przeprowadzona co najwyżej na podstawie badań na działającym systemie. Nie są nam znane żadne tego typu działania, które prowadzone byłyby na systemach w wyżej wymienionych państwach. Wszystkie dostępne statystyki dotyczyły liczby (lub procentowego udziału w rynku) przedsiębiorców telekomunikacyjnych, którzy stosują takie praktyki. Przygotowanie statystki dotyczącej użytkowników i ich zapytań jest co prawda teoretycznie wyobrażalne, ale musiałoby polegać na ingerencji w treść zapytań formułowanych przez użytkowników. Nie ma wątpliwości, że skuteczność blokowania nigdy nie osiągnie 100% stron internetowych o treści uznanej za sprzeczną z prawem. Zasoby internetowe, których adresy zostaną poddane filtrowaniu będą bowiem wciąż dostępne przy pomocy sieci Internet (lub w ramach usług takich jak choćby usług *peer-to-peer*) pod innymi adresami lub przy pomocy innej technologii (przykładowo w związku z istnieniem sieci anonimizujących, połączeń przez VPN, serwerów i usług *proxy*, mechanizmów zmiany adresów IP lub zmiany adresów URL, które eliminują dość skutecznie możliwości blokowania ze strony dostarczycieli usług internetowych bądź operatorów.

8. W 2009 r. rozważano problem utworzenia przez instytucję publiczną bazy danych zawierających adresy konkretnych zasobów (URI), której replika miałaby być kopiowana przez operatorów telekomunikacyjnych i innych dostarczycieli usług internetowych. Podjęto wówczas decyzję, że blokowanie komunikacji *peer-to-peer*, komunikacji w ramach gier on-line (przede wszystkim *MMORPG*) oraz stosowanie technik takich jak *deep packet inspection* jest niewskazane i de facto niemożliwe do zrealizowania. Natomiast w przypadku blokowania dostępu do stron skupiono się na rozwiązaniach typu *BGP* i *DNS blackholing* oraz *URL filtering*. Ta konstatacja ze względów prawnych i technicznych wydaje się do dziś aktualna. Stworzenie bazy konkretnych URI jest oczywiście możliwe i techniczne nawet dość proste. Poza kwestiami związanymi ze skutecznością takiego rozwiązania **wywołuje jednak poważne wątpliwości prawne i ekonomiczne**. Blokowanie adresów IP bądź adresów domenowych będzie bowiem prowadziło do sytuacji, w których blokowane będą wszystkie domeny w ramach tego samego IP, bądź wszystkie poddomeny w ramach tej samej domeny. Taka sytuacja, dziś dużo bardziej popularna niż w 2009 r., musi prowadzić do pojawienia się skomplikowanych problemów cywilnej odpowiedzialności Państwa (oraz operatorów lub dostarczycieli Internetu) za zablokowanie „przy okazji" stron i usług zawierających treści jak najbardziej legalne. Rozwiązaniem mogłoby być prowadzenie bazy URL, ale to rozwiązanie znacząco podnosi koszty po stronie przedsiębiorców telekomunikacyjnych oraz prowadzi do konieczności opisania w prawie funkcji logicznych, jakie wiązać będą URL z pozostałymi identyfikatorami. Wszystkie te rozważania prowadzą do wniosku, że już samo stworzenie bazy nie jest sprawa prostą, a jej utrzymanie będzie wymagało sporych nakładów finansowych i organizacyjnych tak po stronie Państwa jak po stronie przedsiębiorców. Przy kwestionowanej skuteczności takiego rozwiązania koncepcja ta wymaga bardzo dogłębnego rozważenia co do nakładów finansowych jakie trzeba będzie na nią ponieść.

9. Bardzo trudnym problemem, który rozważano w latach 2009-2010 była **kwestia jawności wpisów w takim rejestrze**. Było bowiem oczywiste, że całość rejestru nie może być jawna, bo przecież w ten sposób sama w sobie stanowiłaby unikalnej kolekcje dla nielegalnych linków. Z drugiej strony, w przypadku rynku dostarczycieli usług internetowych, którzy musieliby podporządkować się wymaganiom wynikającym z prawa rozdrobnienie jest znacznie większe niż w przypadku przedsiębiorców telekomunikacyjnych. To oznaczać by mogło, że bardzo drobni dostarczyciele usług internetowych musieliby również „zaciągać" dane z tworzonego rejestru.

Nie ma również wątpliwości, że tak system teleinformatyczny obsługujący taki rejestr jak również komunikacja między uprawnionymi służbami i rejestrem oraz pomiędzy rejestrem a przedsiębiorcami będą obiektem ataków hakerskich wszystkich możliwych typów (od ataków DoS i DDoS po próby modyfikacji lub usunięcia danych). Zakres takich ataków będzie wprost uzależniony od zakresu przedmiotowego blokowania (im szerszy zakres merytoryczny tym większy krąg zainteresowanych atakami oraz tym większy zakres „przyzwolenia społecznego" na dokonywanie takich ataków) oraz od zakresu jawności ewentualnego rejestru (im więcej danych jest jawnych tym większa łatwość przygotowania i przeprowadzenia ataku).

Podsumowując powyższe rozważania Generalny Inspektora Ochrony Danych Osobowych nie uważa, by proponowane przez projektodawców działania Ministra właściwego ds. informatyzacji miały doprowadzić rozwiązania problemu słusznie opisanego w preambule projektu uchwały. Sugerujemy skupienie się na działaniach edukacyjnych w miejsce prac legislacyjnych, które otwierają *puszkę Pandory* cenzury w sieci, wymagają znacznych nakładów, a jednocześnie nie mogą prowadzić do realizacji celu.

2 pozdrawiam