Warszawa, 18 lutego 2012 r.

Szanowny Pan

Michał Boni

Minister Administracji i Cyfryzacji

OPINIA FUNDACJI PANOPTYKON

dotycząca projektu ustawy – Prawo telekomunikacyjne

Ministerstwo Administracji i Cyfryzacji ogłosiło 13 lutego 2012 r. dodatkowe konsultacje w sprawie projektu ustawy – Prawo telekomunikacyjne. Wynika to z wprowadzenia do projektu zmiany dotyczącej zasad retencji danych – skrócenia obowiązkowego okresu przechowywania danych przez operatorów z 24 do 12 miesięcy. Do zmian w tym zakresie odniesiemy się w pierwszej części opinii.

Pierwsze konsultacje projektu ustawy – Prawo telekomunikacyjne odbyły się w sierpniu 2011 r. Fundacja PANOPTYKON przedstawiła wówczas swoją opinię na temat projektu. Przedstawione uwagi zachowały aktualność, dlatego w drugiej części opinii przedstawimy je ponownie.

I. Retencja danych – nierozwiązany problem

Projekt zakłada skrócenie okresu retencji danych telekomunikacyjnych z 24 do 12 miesięcy. Dotychczasowy, dwuroczny okres, był maksymalnym okresem dopuszczalnym przez tzw. dyrektywę retencyjną.

Fundacja PANOPTYKON uważa proponowane rozwiązanie za słuszne, lecz zdecydowanie niewystarczające. Skrócenie okresu retencji danych jest bowiem tylko niewielkim elementem większego problemu. Regulacje dotyczące retencji danych oraz zasad dostępu do nich wymagają gruntownej analizy i przebudowy. Postulowane, najbardziej pilne zmiany dotyczą m.in. zdefiniowania katalogu najpoważniejszych przestępstw, w związku z którymi będzie można korzystać z retencji, ograniczenie kategorii danych, jakie są przechowywane, ograniczenie kręgu podmiotów uprawnionych do dostępu do danych, wprowadzenie zewnętrznej kontroli nad dostępem do danych czy też wprowadzenie obowiązku informacyjnego względem inwigilowanej osoby o czynnościach kontrolnych po ich zakończeniu.

Naszym zdaniem skrócenie okresu retencji do 12 miesięcy nie zostało poparte dostateczną analizą. W uzasadnieniu projektu jest jedynie mowa o tym, że największe znaczenie i wartość mają dane pochodzące z ostatniego roku. Tymczasem zgodnie z Raportem na temat ewaluacji dyrektywy retencyjnej opracowanym przez Komisję Europejską[1] największe uzasadnienie (ze względu na przeanalizowane wzorce wykorzystywania danych w celach dochodzeniowych) ma 6-miesięczny okres retencji. Komisja wskazuje bowiem, że około 90% pobieranych danych przechowywane było 6 miesięcy lub krócej[2].

Należy zwrócić uwagę, że tylko w Polsce wprowadzono obowiązkową retencję wszystkich typów danych telekomunikacyjnych przez maksymalny okres 2 lat. W 15 krajach czas ten wynosi 12 miesięcy, a w trzech (Cypr, Litwa, Luksemburg) 6 miesięcy. Warto również pamiętać, że kilka krajów w ogóle nie wdrożyło dyrektywy retencyjnej i polega wyłącznie na danych przechowywanych przez operatorów w celach komercyjnych (zwykle jest to okres od 3 do 6 miesięcy).

Termin roczny stanowi niejako „wypośrodkowanie" istniejących rozwiązań niepoparte dostateczną analizą, podczas gdy to na państwie (na podstawie art. 31 ust. 3, art. 47 i art. 49 Konstytucji RP) spoczywa obowiązek wykazania, że proponowane ograniczenie prawa do prywatności jest konieczne i proporcjonalne w demokratycznym państwie.

Z powyższych względów w ocenie Fundacji PANOPTYKON okres retencji powinien wynosić 6 miesięcy. Ewentualnie, można poddać pod rozwagę zróżnicowanie czasu retencji w zależności od rodzaju zatrzymywanych danych, np. ustalić inne okresy zatrzymywania dla danych o komunikacji telefonicznej i internetowej[3].

W opiniowanym projekcie brak jest nie tylko odpowiednich zmian w ustawach kompetencyjnych. Naszym zdaniem nowelizując samo Prawo telekomunikacyjne ustawodawca powinien wzmocnić ochronę prywatności poprzez:

1. Wprowadzenie do ustawy – Prawo telekomunikacyjne obowiązku chociażby częściowego zwrotu kosztów ponoszonych przez operatorów w związku z realizacją ich obowiązków w zakresie retencji danych. Wprowadzenie tego obowiązku ma znaczenie nie tylko dla interesów ekonomicznych operatorów, ale przede wszystkim dla poszanowania zasady niezbędności i proporcjonalności. Wprowadzenie przynajmniej częściowej rekompensaty – obciążającej budżet podmiotów, które o dane występują – przeciwdziałałoby sięganiu po dane retencyjne w sytuacjach nieuzasadnionych. Stanowiłoby to swoistą „zachętę do samoograniczania się" przez służby.

2. Rozbudowanie przepisów dotyczących sprawozdawczości. Obecnie Urząd Komunikacji Elektronicznej dostaje tylko ogólne dane od samych operatorów (ile zapytań od wszystkich uprawnionych organów było w danych roku), nie ma natomiast żadnej możliwości zweryfikowania, jakie konkretnie organy i w jakich celach pobierają konkretne rodzaje danych telekomunikacyjnych.

---

[1] Report From the Commission to the Council And The European Parliament: Evaluation report on the Data Retention Directive (COM(2011) 225 final).

[2] Raport nie zawiera wyrażonej wprost propozycji optymalnego okresu retencji. Z przedstawionych w nim danych wynika jednak, że uzasadnione jest przechowywanie danych przez 6 miesięcy. Tymczasem uzasadnienie opiniowanego projektu powołuje bezzasadnie Raport Komisji jako uzasadnienie skrócenia okresu retencji do 12 miesięcy.

[3] Takie rozwiązanie przyjęto w Słowenii.

W zakresie problemu retencji danych należy wskazać jeszcze na wprowadzone w projekcie ograniczenie prawa ujawniania „komunikatów i danych" objętych tajemnicą telekomunikacyjną do sytuacji, w których postanowienie w tym przedmiocie wyda **sąd karny** (art. 159 ust. 4), a nie – jak dotychczas – każdy sąd. Zmiana ta, zgodnie z przedstawionym uzasadnieniem projektu nowelizacji, ograniczyć ma niedopuszczalne w odniesieniu do ochrony przed nadmierną ingerencją w prawa i wolności obywatelskie, korzystanie z dostępu do danych retencyjnych na użytek postępowań cywilnych.

Sprecyzowanie w art. 159 ust. 4, że tajemnica telekomunikacyjna nie dotyczy danych ujawnionych postanowieniem sądu wydanym jedynie w postępowaniu karnym oceniamy pozytywnie. Jednocześnie zwracamy uwagę na to, że zasady dostępu sądów cywilnych do danych objętych tajemnicą telekomunikacyjną wymagają precyzyjnej regulacji. Tymczasem, pomimo wprowadzanych zmian, wciąż niejasne pozostaje kiedy i w jakim zakresie sądy cywilne mogą sięgać po te dane.

II. **Pozostałe zmiany**

A. **Zgoda na używanie plików *cookies***

Na szczególną uwagę zasługuje propozycja zmiany **art. 173 ust. 1** Prawa telekomunikacyjnego, rozszerzająca zakres obowiązków informacyjnych podmiotów świadczących usługi drogą elektroniczną oraz przedsiębiorców telekomunikacyjnych związanych z przechowywaniem danych informatycznych w urządzeniach końcowych abonenta lub użytkownika końcowego oraz uzyskiwaniem dostępu do tych danych. Konieczność znowelizowania art. 173 Prawa telekomunikacyjnego i zasad dostępu do plików *cookies* wynika z obowiązku implementacji zmian wprowadzonych w art. 5 ust. 3 dyrektywy 2002/58/WE o prywatności i łączności elektronicznej (dalej: „dyrektywa").

Zaproponowane zmiany niewątpliwie pomogą bardziej efektywnie chronić prawa użytkowników sieci. Przewidziane rozwiązania uważamy jednak za **niewystarczające**. Nasze zastrzeżenia dotyczą w szczególności rezygnacji projektodawcy z przyjętego w dyrektywie modelu *opt-in* w zakresie wyrażenia zgody na przechowywanie i uzyskiwanie dostępu do plików *cookies.*

Wbrew argumentacji przedstawionej w uzasadnieniu projektu nowelizacji, proponowane zmiany w przepisach nie gwarantują, w naszej ocenie, wystarczającego poziomu ochrony prywatności użytkowników Internetu. W szczególności, jeżeli pliki typu *cookies* są przetwarzane np. w związku z celami marketingowymi podmiotów trzecich, umożliwiając im profilowanie internautów i rejestrowanie ich codziennej aktywności w sieci.

Przyjęcie, że rozszerzone obowiązki informacyjne po stronie usługodawców spowodują w sposób automatyczny, że użytkownicy będą w sposób bardziej świadomy „obsługiwać" pliku typu *cookies* jest niebezpieczną fikcją. Badania pokazują, że niewielu użytkowników Internetu, poruszając się po sieci, poświęca czas na modyfikowanie narzuconych „odgórnie" ustawień prywatności i odpowiednią konfigurację przeglądarek internetowych[4]. Jednocześnie poczucia zagrożenia związane z ochroną prywatności w Internecie wzrasta – problem naruszeń prywatności w sieci staje się coraz powszechniej dostrzegalny, o czym świadczy choćby liczba skarg do Generalnego Inspektora Ochrony

[4]Polskie Badania Internetu: *Coraz więcej odsłania się w sieci*, Rzeczpospolita, 5 maja 2011 r. http://www.rp.pl/artykul/17,652931.html; *Dzieci bez prywatności w sieci*, Rzeczpospolita, 19 kwietnia 2011 r., http://www.rp.pl/artykul/17,645674.html.

Danych Osobowych dotyczących Internetu, która w 2010 r. uległa podwojeniu w stosunku do 2009 r.[5].

W tym świetle, poważne wątpliwości wzbudza teza zaprezentowana w uzasadnieniu projektu nowelizacji, zakładająca „niezwykłą łatwość w dokonaniu przez abonenta lub użytkownika końcowego zmian w ustawieniach przeglądarki uniemożliwiających przechowywanie i uzyskiwanie dostępu do wprowadzonych danych przez podmioty zewnętrzne". Przywołane wyżej badania wskazują na przeciwną konkluzję, jeśli chodzi o świadomość internautów, co do sposobów ochrony przed zagrożeniami związanymi z nadużyciami prawa do prywatności *on-line.* Co więcej, trudno oczekiwać, aby świadomość „statystycznego użytkownika" Internetu w pełni nadążała za szybkim rozwojem technologicznym, który postępuje także w odniesieniu do ciągłej ewolucji plików typu *cookies* (tworzone są nowe rodzaje *cookies*, których nie można zablokować z poziomu przeglądarki; Raport Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji ENISA wskazuje na widoczny trend wśród internetowych reklamodawców na stosowanie coraz bardziej inwazyjnych narzędzi śledzenia internautów[6]).

W związku z tym uważamy za niezbędne wprowadzenie modelu wyrażania zgody w trybie *opt-in*. Użytkownicy Internetu powinni mieć zagwarantowaną nie tylko możliwość zgłoszenia sprzeciwu, ale przede wszystkim prawo do <u>niewyrażenia</u> zgody. Utrzymanie zgody jako „opcji domyślnej" nie zapewnia pełnej świadomości korzystania z usług internetowych związanych z korzystaniem z plików *cookies*. Dlatego też, w naszej ocenie, projektodawca powinien rozważyć rezygnację z utrzymania zgody domniemywanej z braku sprzeciwu i wprowadzić obowiązek jej uprzedniego uzyskania przez usługodawców.

Aby uniknąć zagrożeń i niedogodności związanych z ograniczeniem działalności podmiotów gospodarczych korzystających z *cookies,* należy jednocześnie założyć, że wyraźna zgoda wyrażona w trybie *opt-in* nie musi dotyczyć każdego konkretnego pliku, ale może być generyczna (dotyczyć danego rodzaju pliku *cookies* lub danego usługodawcy). Taki model testują obecnie z powodzeniem twórcy najbardziej popularnych przeglądarek internetowych[7].

W dodatku, mimo zapewnień przedstawionych w uzasadnieniu projektu nowelizacji, poważne wątpliwości budzi to, czy pozostawienie modelu *opt-out* daje się w istocie pogodzić ze zmienioną treścią art. 5 ust. 3 dyrektywy. Przepis dyrektywy mówi wyraźnie: „Państwa członkowskie zapewniają, aby przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika było dozwolone wyłącznie pod warunkiem, że dany abonent lub użytkownik wyraził zgodę zgodnie z dyrektywą 95/46/WE po otrzymaniu jasnych i wyczerpujących informacji, między innymi o celach przetwarzania". Wydaje się zatem, że jasny przekaz płynący z art. 5 ust. 3 nie pozostawia miejsca na dość swobodną interpretację „intencji dyrektywy", jakiej dokonano w uzasadnieniu projektu nowelizacji oraz na zastosowanie dowolnych środków, ale narzuca wprowadzenie rozwiązań przewidzianych wprost w implementowanym akcie

---

[5] *Boimy się o swoją prywatność: rekordowa ilość skarg do głównego inspektora ochrony danych osobowych*, Dziennik Gazeta Prawna, 11 kwietnia 2011 r., http://prawo.gazetaprawna.pl/artykuly/503892,boimy_sie_o_swoja_prywatnosc_rekordowa_ilosc_skarg_do_glownego_inspektora_ochrony_danych_osobowych.html.

[6] http://www.enisa.europa.eu/act/it/eid/xborderauth/at_download/fullReport.

[7] Zob. np. *IE9 and Privacy: Introducing Tracking Protection*, http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx lub *Some Technical Clarifications About Do Not Track*, https://freedom-to-tinker.com/blog/harlanyu/some-technical-clarifications-about-do-not-track.

prawnym. Gdyby intencją ustawodawcy europejskiego było pozostawienie tak dużego marginesu swobody organom krajowym w tym zakresie, nie zakreśliłby w tekście dyrektywy konkretnego modelu wyrażania zgody.

Warto ponadto podkreślić, że za modelem wyrażania zgody w trybie *opt-in* opowiedziała się Grupa Robocza Artykułu 29 (ciało doradcze złożone z organów ochrony danych osobowych wszystkich państw członkowskich Unii Europejskiej). W opinii przedstawionej 22 czerwca 2010 r.[8], Grupa Robocza „wzywa operatorów sieci reklamowych do utworzenia mechanizmów uprzedniej zgody (*opt-in*), wymagających aktywnego potwierdzenia ze strony osób, których dane dotyczą, na przyjęcie plików *cookies* lub podobnych narzędzi oraz na późniejsze monitorowanie ich zachowania podczas przeglądania Internetu do celów wyświetlania dopasowanych reklam". Ponadto, utrzymanie modelu *opt-out* stałoby w sprzeczności z koncepcją „prywatności jako opcji domyślnej" (ang. *privacy by default*), która, zgodnie ze stanowiskiem Komisji Europejskiej[9], będzie jedną z fundamentalnych zasad, na których opierać się będzie zapowiedziana w styczniu 2010 r. reforma systemu ochrony danych osobowych w Unii Europejskiej[10].

B. Zawiadomienie o naruszeniu bezpieczeństwa danych osobowych

Z aprobatą przyjmujemy wprowadzenie w projekcie nowelizacji **art. 174a**, przewidującego obowiązek zawiadomienia przez usługodawcę telekomunikacyjnego o przypadkach naruszenia danych osobowych abonentów lub użytkowników końcowych. Jest to niewątpliwie krok w dobrym kierunku, który gwarantuje abonentom i użytkownikom końcowym prawo do informacji o tym, w jaki sposób przetwarzane są ich dane i wzmacnia tym samym mechanizmy ochronne zmierzające do zapewnienia bezpieczeństwa osobom korzystającym z Internetu. W szczególności świadomość, że o naruszeniu zostaną powiadomieni usługobiorcy, może wywołać korzystny skutek „samokontroli" usługodawców, którzy być może staną się bardziej skłonni do tego, aby powstrzymać się od stosowania złych praktyk w obawie przed utratą zaufania odbiorców swoich usług.

Wątpliwości budzi jednak wyłączenie przewidziane w projektowanym **art. 174a ust. 3.** Szczególnie, że objaśnienie celowości tegoż wyłączenia zostało całkowicie pominięte w uzasadnieniu projektu nowelizacji. Stoimy na stanowisku, że **w każdej sytuacji, gdy „naruszenie danych osobowych może wywrzeć niekorzystny wpływ na dane osobowe lub prywatność abonenta lub użytkownika końcowego", powinien być utrzymany obowiązek jego powiadomienia, nawet wówczas, gdy „usługodawca wdrożył odpowiednie techniczne środki ochrony danych osobowych".**

Nasze wątpliwości budzi również brak określenia konkretnego terminu na zawiadomienie o naruszeniu danych osobowych abonentów lub użytkowników końcowych, zarówno w przypadku obowiązku zawiadomienia abonentów/użytkowników (ust. 2), jak i Generalnego Inspektora Ochrony Danych Osobowych (ust. 1). Odwołanie się w proponowanych przepisach do klauzuli generalnej „bez zbędnej zwłoki" uważamy w tym przypadku za niewystarczające i mogące poważnie ograniczyć skutki oddziaływania proponowanej regulacji.

---

[8] Opinia 2/2010 w sprawie internetowej reklamy behawioralnej, http://www.mi.gov.pl/files/0/1793926/wp171plopiniagrupyochronydanychosobowychreklamabehawioralna.pdf.

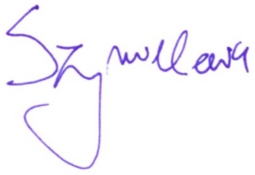
[9] Zob. przemówienie Komisarz ds. sprawiedliwości wymiaru sprawiedliwości i obywatelstwa w Komisji Europejskiej Viviane Reding do Parlamentu Europejskiego z 16 marca 2011 r., http://www.euractiv.com/en/infosociety/reding-defines-new-eu-data-privacy-rules-news-503172.

[10] Zob. Komunikat KE z 4 listopada 2010 r. pt. „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", http://www.panoptykon.org/sites/default/files/com_2010_609_pl-1.pdf.

III. **Uwagi końcowe**

Fundacja PANOPTYKON podjęła decyzję o złożeniu powyższej opinii za pośrednictwem strony internetowej Ministerstwa Administracji i Cyfryzacji rezygnując z wykorzystywania portalu mamzdanie.org.pl. Nasze zastrzeżenia budzi bowiem charakter i regulamin tego portalu. Współwłaścicielem portalu jest spółka z ograniczoną odpowiedzialnością, a regulamin jest w wielu punktach sprzeczny z wartościami, jakie powinny być chronione w konsultacjach społecznych (m.in. przewiduje możliwość wprowadzenia odpłatności za świadczone usługi oraz przejęcie majątkowych praw autorskich do wszelkich treści publikowanych przez użytkowników). Wskazuje to na komercyjny charakter tego przedsięwzięcia.

W imieniu Fundacji PANOPTYKON,



Katarzyna Szymielewicz

Prezes Fundacji Panoptykon