Warszawa, 2 sierpnia 2011 r.

**Pani Magdalena Gaj**
**Podsekretarz Stanu**
**Ministerstwo Infrastruktury**

# Uwagi Fundacji PANOPTYKON do projektu ustawy o zmianie ustawy Prawo telekomunikacyjne i niektórych innych ustaw

W nawiązaniu do pisma Ministerstwa Infrastruktury z 18 lipca 2011 r. (sygn. ŁT3c-020-42/11), Fundacja PANOPTYKON pragnie przedstawić uwagi do przedłożonego w ramach prowadzonych konsultacji społecznych projektu ustawy o zmianie ustawy Prawo telekomunikacyjne i niektórych innych ustaw (dalej: „projekt nowelizacji"). Przedstawione uwagi koncentrują się na tych aspektach nowelizacji, które w sposób najbardziej bezpośredni związane są z celami statutowymi Fundacji.

## I. Zgoda na używanie plików *cookies*

Na szczególną uwagę zasługuje propozycja zmiany **art. 173 ust. 1** Prawa telekomunikacyjnego[1], 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.

[1] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r., nr 171, poz. 1800 z późn. zm.).

Przyjęcie, że rozszerzone obowiązki informacyjne po stronie usługodawców spowodują w sposób automatyczny, że użytkownicy będą w bardziej świadomie „obsługiwać" pliki 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[2]. 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 Danych Osobowych dotyczących Internetu, która w 2010 r. uległa podwojeniu w stosunku do 2009 r.[3].

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: stosowanie coraz bardziej inwazyjnych narzędzi śledzenia internautów[4]).

**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[5].

W dodatku, mimo zapewnień przedstawionych w uzasadnieniu projektu nowelizacji, poważne wątpliwości budzi to, czy pozostawienie modelu *opt-out* daje się pogodzić ze

---

[2] 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.

[3] *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.

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

[5] 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.

zmienioną treścią art. 5 ust. 3 dyrektywy. Przepis dyrektywy mówi wyraźne: „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 prawnym. Gdyby intencją prawodawcy 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.[6], 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[7], będzie jedną z fundamentalnych zasad, na których opierać się będzie zapowiedziana w styczniu 2010 r. reforma systemu ochrony danych osobowych w Unii Europejskiej[8].

**II. 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**

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

[7] 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.

[8] 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.

**"naruszenie danych osobowych może wywrzeć niekorzystny wpływ na dane osobowe lub prywatność abonenta lub użytkownika końcowego", powinien być utrzymany obowiązek jego powiadomienia, nawet wówczas, jeśli „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.

## III. Ochrona tajemnicy telekomunikacyjnej

Na wstępie, chcielibyśmy podkreślić, że z aprobatą przyjmujemy proponowane w punkcie 116 projektu nowelizacji poszerzenie definicji „danych transmisyjnych" o dane "wskazujące położenie geograficzne urządzenia końcowego" wygenerowane także „w ramach usług telekomunikacyjnych" **(art. 159 ust. 1 pkt 3)**. Propozycja ta oznacza wzmocnienie gwarancji wynikających z tajemnicy telekomunikacyjnej oraz odpowiada rozwojowi rynku usług telekomunikacyjnych (np. typu Facebook, czy Foursquare).

Pozytywnie oceniamy również wprowadzone w projekcie ustawy 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 wynika to z obecnie obowiązujących przepisów – 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 prowadzonych postępowań cywilnych.

W kontekście rozpoczętej w zeszłym roku debaty publicznej dotyczącej przepisów regulujących zasady retencji danych telekomunikacyjnych oraz krytycznej analizy obowiązujących regulacji przedstawionej przez liczne instytucje (m.in. Rzecznika Praw Obywatelskich[9], Naczelną Radę Adwokacką[10], Komisję Europejską[11] czy organizacje pozarządowe), trudno wprowadzane projektem nowelizacji zmiany zwiększające ochronę danych objętych tajemnicą telekomunikacyjną, określić inaczej, niż jako zmiany jedynie „kosmetyczne" i **niewystarczające w kontekście innych przepisów Prawa telekomunikacyjnego**. Tak długo, jak pozostaną w mocy obecne zasady dotyczące retencji danych (przede wszystkim art. 180a Prawa telekomunikacyjnego) zasadniczy problem – niekontrolowanego dostępu do gromadzonych danych przez służby i inne organy, w tym sądy cywilne – pozostaje nierozwiązany.

Potrzebna jest zatem kompleksowa rewizja postanowień Prawa telekomunikacyjnego, a także przepisów zawartych w odrębnych ustawach regulujących dostęp i korzystanie z przechowywanych przez usługodawców danych telekomunikacyjnych (czyli w „ustawach

[9] Zob. Wystąpienie generalne RPO do Prezesa Rady Ministrów Donalda Tuska z dnia 17 stycznia 2011 r., http://www.sprawy-generalne.brpo.gov.pl/pdf/2010/12/662587/1540465.pdf.

[10] Raport NRA pt. *Retencja danych: troska o bezpieczeństwo czy troska o obywateli?* http://adwokatura.pl/wp-content/uploads/2011/05/Raport-pdf.pdf

[11] Zob. raport Komisji Europejskiej z 18 kwietnia 2011 r. dotyczący ewaluacji implementacji dyrektywy retencyjnej http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf.

kompetencyjnych" regulujących uprawnienia poszczególnych służb, czy w Kodeksie postępowania karnego). Postulowane, najbardziej pilne zmiany dotyczą m.in. zdefiniowania katalogu najpoważniejszych przestępstw, przy których będzie można korzystać z retencji; ograniczenia kategorii danych, jakie są przechowywane; ograniczenia kręgu podmiotów uprawnionych do dostępu do danych; wprowadzenie zewnętrznej kontroli nad dostępem do danych, wprowadzenia obowiązku informacyjnego względem inwigilowanej osoby o czynnościach kontrolnych po ich zakończeniu; czy też skrócenie czasu przechowywania danych przez operatorów. Potrzebę zmian sygnalizują w swoich stanowiskach wszystkie wymienione wyżej instytucje. Znajduje ona swój wyraz również w „Raporcie dotyczącym retencji danych telekomunikacyjnych" przedstawionym 4 lipca 2011 r. przez Jacka Cichockiego, Sekretarza Kolegium ds. Służb Specjalnych przy Kancelarii Prezesa Rady Ministrów[12].

W imieniu Fundacji PANOPTYKON

Małgorzata Szumańska
Członkini Zarządu

[12] http://bip.kprm.gov.pl/kprm/komunikaty/281_4067.html.