Raport z prac warsztatów ds. ochrony prywatności

Przedmiotem zainteresowania grupy jest ochrona danych osobowych i prywatności w sieciach telekomunikacyjnych, głównie sieci Internet. Uczestnicy spotkali się w miesiącach kwiecień-maj trzykrotnie, dyskutując o najpilniejszych kwestiach dotyczących procedowanych równolegle przepisów (prawo telekomunikacyjne), działań zmierzających do implementacji przepisów dyrektywy 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW, w tym kontrowersyjnego przepisu art. 25 dyrektywy.

Bloki tematyczne

Pracę w ramach grupy podzieliliśmy na następujące bloki tematyczne, które wraz z kwestiami szczegółowymi, zostały uprzednio zidentyfikowane przez współprzewodniczących grupy (Fundacja Panoptykon/MAC) jako najważniejsze, na chwilę obecną, do omówienia. Wszyscy zaproszeni eksperci otrzymali niniejsze zagadnienia przed spotkaniami grupy.

1. Zasady i cele przechowywania danych telekomunikacyjnych (obowiązek retencji; art. 168 ustawy Prawo telekomunikacyjne):

2. Profilowanie użytkowników i reklama behawioralna/cookies:

a) Czy profilowanie użytkowników w Internecie, jako złożony problem, wymaga odpowiedzi regulacyjnej?
b) Jaki jest pożądany poziom informacji i sposób ich dostarczenia użytkownikowi, zanim podejmie on decyzję o wyrażeniu zgody na profilowanie? Czy niezbędne jest w tym zakresie wprowadzenie nowych lub modyfikacja już obowiązujących reguł postępowania w relacji z klientem?
c) Czy zasadne jest wprowadzenie modelu opartego na samoregulacji, jeżeli tak – pod egidą jakiego organu?
d) Czy możliwe jest przeciwdziałanie nielegalnemu profilowaniu, takiemu na które użytkownik nie wyraził zgody lub nie jest takich działań świadomy? Jeżeli tak – jaki organ i w jaki sposób mógłby efektywnie przeciwdziałać tego rodzaju praktykom?
e) Jak rozumieć wyłączenie obowiązku uzyskania zgody, o którym mowa w art. 173 ust. 2 ustawy Prawo telekomunikacyjne? Czy takie wyłączenie nie będzie stanowić klucza do obejścia obowiązku uzyskania wyraźnej zgody przez usługodawcę? Jakie są granice "niezbędności" i kto ma o tym rozstrzygać w praktyce?
f) W jaki sposób (biorąc pod uwagę aspekty techniczne) należy w praktyce zagwarantować klientowi możliwość wyrażenia zgody na otrzymywanie cookies? Czy można do tego celu wykorzystać ustawienia przeglądarki albo rozwiązania takie jak TPL lub DNT?
g) W jaki sposób możemy skutecznie ograniczyć stosowanie nowych typów cookies (supercookies, evercookies, flashcookies, ubercookies etc.), które już w dniu dzisiejszym wydaje się być niezgodne z obowiązującymi przepisami, w tym kodeksu karnego w zakresie przestępstw przeciwko ochronie informacji (cache sniffing, XSS cookie sniffing etc.)?
h) Czy możliwe jest wypracowanie na zasadzie samoregulacji takich mechanizmów, które ułatwiałyby pozyskanie zgody w sposób minimalizujący uciążliwość dla użytkownika, a jednocześnie gwarantowałyby mu pełną kontrolę nad przetwarzanymi danymi?

3. Monitoring aktywności w sieci telekomunikacyjnej, dostęp do i filtrowanie danych objętych tajemnicą telekomunikacyjną (neutralność sieci/ zarządzanie ruchem/ ochrona sieci i usług telekomunikacyjnych):

a) Projektowany art. 175c ustawy Prawo telekomunikacyjne ma na celu zapewnienie bezpieczeństwa sieci i usług telekomunikacyjnych. A zatem tylko w takim zakresie i celu przedsiębiorca telekomunikacyjny będzie mógł podejmować działania ograniczające prawa użytkowników. Czy istnieje zagrożenie nadużywania tego przepisu?
b) Czy możliwe jest uprzednie i przejrzyste zdefiniowanie działań, jakie przedsiębiorca telekomunikacyjny będzie zobowiązany podejmować na podstawie tego przepisu?
c) Jakie, jeżeli w ogóle, problemy związane z przetwarzaniem danych osobowych lub ochroną prywatności może powodować stosowanie tego przepisu?
d) Czy konieczna jest modyfikacja obecnego brzmienia projektowanego przepisu, mając na uwadze to, że stanowi on implementację przepisu art. 13a dyrektywy ramowej?

4. Blokowanie treści – dyrektywa w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej (art. 25 ust. 2):

a) Przepis art. 25 ust. 2 wspomnianej dyrektywy jest fakultatywny i daje państwom członkowskim możliwość podejmowania określonych działań. Czy potrzebne i możliwe jest wprowadzanie w polskim prawie obowiązku blokowania treści pedofilskich?
b) Jakie są dostępne metody blokowania, jak przedstawia się relacja skuteczności do kosztów oraz analiza "kosztów" prawnych i społecznych?
c) Czy możliwe jest efektywne blokowanie tego rodzaju materiałów w sieci Internet bez naruszania praw innych podmiotów?
d) Czy możliwe jest zwiększenie efektywności ścigania i usuwania stron zawierających lub rozpowszechniających pornografię dziecięcą utrzymywanych na terytorium RP?

Uczestnicy grupy warsztatowej

Niestety, ze względów praktycznych, nie mogliśmy do bezpośredniego udziału w pracach zaprosić wszystkich chętnych. Biorąc pod uwagę konieczność wypracowania konkluzji we wszystkich blokach tematycznych, postaraliśmy się jednak o to, żeby każda z możliwych grup interesariuszy była w pracach reprezentowana:

- ✓ Zbigniew Braniecki (Mozilla)
- ✓ Mirosław Wróblewski/Katarzyna Łakomiec (RPO)
- ✓ Agata Wacławik-Wejman (Google)
- ✓ Jakub Pepłoński (Allegro)
- ✓ Grzegorz Wanio (Kancelaria Olesiński i Wspólnicy/Nasza Klasa)
- ✓ Maciej Pajęcki (Nasza Klasa)
- ✓ Piotr Drobek/Tomasz Soszyński (GIODO)
- ✓ Mariusz Grzesiuk (Grupa Onet)
- ✓ Barbara Chrzczonowska (Orange)
- ✓ Marek Szydłowski (Kancelaria Wardyński i Wspólnicy)
- ✓ Michał Woźniak (Fundacja Wolnego i Otwartego Oprogramowania)

- ✓ Mirosław Maj (Fundacja Bezpieczna Cyberprzestrzeń)
- ✓ Marek Jurkiewicz (UKE)
- ✓ Katarzyna Szymielewicz (Fundacja Panoptykon)
- ✓ Małgorzata Szumańska (Fundacja Panoptykon)
- ✓ Beata Dobrzyńska-Borucka (MAC)
- ✓ Agnieszka Jędrzejczyk (MAC)
- ✓ Dariusz Dąbek (MAC)

Dodatkowo, ze względu na tematykę trzeciego spotkania obejmującą monitoring w sieci oraz możliwości techniczne wprowadzenia obowiązku blokowania dostępu do treści pedofilskich, zaprosiliśmy do udziału ekspertów:

- ✓ Tomasz Piłat (Orange)
- ✓ Sławomir Pijanowski (Orange)
- ✓ Maciej Łopaciński (Agora TC Sp. z o.o.)
- ✓ Piotr Szeptyński (t-mobile)
- ✓ Janusz Górski (t-mobile)
- ✓ Maciej Kołodziej (ABI, Nasza Klasa)

Zaproszenie do prac wystosowaliśmy również do następujących osób, które jednak z różnych względów nie wzięły udziału w spotkaniach:

- ✓ Jozef Halbersztadt (ISOC)
- ✓ Grzegorz Sibiga (Zakład Prawa Administracyjnego. Instytut Nauk Prawnych PAN)
- ✓ Adam Haertle (UPC)
- ✓ Piotr Marczuk (Microsoft)
- ✓ Jacek Urban (osoba prywatna)
- ✓ Jarosław Mojsiejuk (Cyfrowy Polsat)

Pierwsze spotkanie – blok tematyczny Nr 2 Profilowanie użytkowników, reklama behawioralna i cookies

Jako pierwsze, ze względu na równoczesne prace nad projektem nowelizacji ustawy Prawo telekomunikacyjne i prośbę Ministra Igora Ostrowskiego, omówione zostały kwestie związane z implementacją do polskiego porządku prawnego przepisu art. 5 ust. 3 znowelizowanej dyrektywy 2002/58/WE (tzw. dyrektywa o prywatności). Dyskusja sprowadziła się w związku z tym do analizy wymogu uzyskania zgody na przetwarzanie cookies, sposobu wyrażenia zgody (np. za pomocą ustawień przeglądarki), uprzedniego charakteru obowiązku informacyjnego względem użytkownika, świadomości użytkownika co do celów i sposobów przetwarzania cookies etc. Z tego względu zakładana agenda spotkania nie została w pełni zrealizowana.

ZGODA A SPRZECIW UŻYTKOWNIKA

Stosownie do postanowień znowelizowanego art. 5 ust. 3 dyrektywy o prywatności, niezbędne jest dokonanie w treści art. 173 ustawy Prawo telekomunikacyjne odpowiednich zmian. Główna zmiana polega na zastąpieniu możliwości przetwarzania cookies do momentu wyrażenia przez użytkownika sprzeciwu (tzw. opcja opt-out), zgodą użytkownika (tzw. opcja opt-in). W toku dyskusji

przedstawiciele biznesu zwrócili uwagę na brzmienie motywu 66 dyrektywy o prywatności, w którym ustawodawca europejski podkreśla ogromne znaczenie konieczności przekazywania użytkownikom jasnych i wyczerpujących informacji, gdy podejmują jakiekolwiek działania, które mogłyby skutkować nieuprawnionym przechowywaniem lub dostępem. Jednocześnie ustawodawca europejski zwraca uwagę na to, że metody udostępniania informacji oraz oferowania prawa do odmowy powinny być jak najbardziej przyjazne dla użytkownika.

- Uczestnicy zwrócili uwagę na fakt niespójności przepisu dyrektywy, w którym mówi się o zgodzie, z brzmieniem korespondującego motywu 66, w którym mówi się naprzemiennie o sprzeciwie i o zgodzie.
- Dyskusja prowadziła do wniosku, że kluczową kwestią, która w debacie publicznej jest często przysłonięta przez formalistycznie traktowaną alternatywę między dwoma modelami regulacji: opartym na sprzeciwie (opt-out) i opartym na zgodzie (opt-in), jest samo zdefiniowanie pojęcia „świadomej zgody użytkownika" na przetwarzanie cookies.
- Był to pierwszy punkt zapalny w dyskusji, w której zarysowały się dwa przeciwstawne stanowiska:
  - zgoda może być wyrażona również poprzez brak jakiejkolwiek akcji ze strony użytkownika w sytuacji, gdy użytkownik jest odpowiednio poinformowany o prawnych skutkach niepodjęcia działania (tzw. strona biznesowa);
  - na gruncie przepisów dyrektywy o prywatności w komunikacji elektronicznej, która wyraźnie odsyła w tym zakresie do dyrektywy 95/46[1], tylko wyraźne działanie podjęte przez użytkownika można uznać za akt wyrażenia świadomej zgody (przedstawiciele GIODO oraz Fundacji Panoptykon).

ŚWIADOMOŚĆ UŻYTKOWNIKA

Niezależnie od powyższego uczestnicy spotkania zwrócili uwagę na fakt, iż w przypadku cookies, od strony usługodawcy trudno jest mówić o zgodzie konkretnego użytkownika, gdyż usługodawca przetwarza dane z urządzenia końcowego, z którego może korzystać kilku użytkowników i nie jest możliwe spersonalizowanie każdego z nich z osobna.

- Już z tego powodu relacja wspomnianych wyżej dyrektyw wydała się uczestnikom niespójna, skoro usługodawca w większości przypadków nie jest w stanie zidentyfikować osoby korzystającej z komputera lub smartfonu, w związku z czym nie ma możliwości pozyskać zgody odpowiadającej wymogom dyrektywy 95/46.

USTAWIENIA PRZEGLĄDARKI

Przedyskutowano również możliwość wyrażenia zgody przez użytkownika za pomocą ustawień przeglądarki. Uczestnicy zwrócili uwagę na doświadczenia innych państw członkowskich, które dokonały już implementacji wspomnianego przepisu dyrektywy o prywatności. Nie było możliwe ustalenie, czy poszczególne prawa narodowe w tym zakresie odnoszą się do zgody rozumianej jako działanie podjęte przez użytkownika, zgody rozumianej jako akt woli, który nie musi być wyrażony żadnym działaniem, czy jedynie do możliwości wyrażenia sprzeciwu[2]. Natomiast zidentyfikowano

[1] Dyrektywa w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Zgodnie z brzmieniem art. 2 lit. h dyrektywy 95/46, zgoda osoby, której dane dotyczą oznacza konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych.

[2] Sprzeczne informacje w tym zakresie należy wskazać w dwóch opracowaniach, których celem jest monitorowanie stanu implementacji przepisu art. 5 ust. 3 dyrektywy o prywatności:

sygnalizację niektórych państw członkowskich (np. Wielka Brytania[3], Francja[4]), iż na chwilę obecną brak jest na rynku przeglądarek, które umożliwiałyby pozyskanie zgody użytkownika w sposób odpowiadający wymogom dyrektywy 95/46. Z tego powodu zaleca się stosowanie „innych rozwiązań informatycznych" (np. plug-in-ów do przeglądarek) lub wprost przykładowo wskazuje się sposoby odpowiedniego pozyskania zgody[5].

! Pojawił się wniosek (ze strony przedstawicieli biznesu), że w związku z brakiem możliwości zapewnienia dostępności przeglądarek lub innych odpowiednich rozwiązań informatycznych o podobnej funkcjonalności przy pomocy rozwiązań legislacyjnych, kwestia ta powinna być „regulowana" przez sam rynek. Z drugiej strony pojawił się głos ze strony przedstawiciela Mozilli dotyczący możliwości szybkiego wdrożenia odpowiednich rozwiązań technicznych (vide poniżej).

KONKLUZJE I REKOMENDACJE

1. Nie ma możliwości „pogodzenia" stanowisk biznesu i organizacji społecznych, w związku z czym sygnalizowane są one jako odrębne i pozostają aktualne. Mamy do czynienia z konfliktem prawa do prywatności i swobody prowadzenia działalności w Internecie. Jakakolwiek będzie w tym zakresie decyzja, niezbędne jest zachowanie równowagi między tymi wartościami. Dylemat co do tego, jak uzyskać taki stan równowagi albo jakie wartości należy poświęcić, powinien być rozstrzygnięty w drodze decyzji politycznej.
2. Zgodnie ze stanowiskiem zaprezentowanym przez przedstawiciela Mozilli, wszyscy dostawcy przeglądarek są w stanie zaimplementować rozwiązania umożliwiające pozyskanie zgody użytkownika w przeciągu 18 tygodni.
3. Profilowanie użytkowników jest dzisiaj powszechne: w relacjach z biznesem reklamowym traktowani są oni jak „produkt", a nie jak myślący podmiot.
4. Strona biznesowa jest zwolennikiem samoregulacji oraz intuicyjnych narzędzi dla użytkownika.
5. Strona organizacji społecznych stoi na stanowisku, że przyjęcie modelu opt-in, opartego na świadomej i wyraźnej zgodzie użytkownika, która jednocześnie może być wyrażona za pomocą ustawień przeglądarki, będzie właściwą implementacją dyrektywy, jak również zapewni użytkownikom lepszy poziom poinformowania w zakresie rodzajów, celów i zasad działania cookies.

Drugie spotkanie – blok tematyczny Nr 1
Zasady i cele przechowywania danych telekomunikacyjnych

Dyskusję nad zagadnieniami zachowywania i udostępniania danych telekomunikacyjnych można podzielić na kilka obszarów, wśród których wyróżnić należy zasadność obowiązkowej retencji, kontrolę pozyskiwania i przetwarzania danych, obowiązki informacyjne dla obywateli, odpłatność za pozyskanie danych oraz kwestię szczególnej ochrony tajemnic zawodowych (lekarskiej, adwokackiej, dziennikarskiej etc.).

---

http://www.ffw.com/pdf/cookie-consent-tracking-table.pdf.
http://www.twobirds.com/English/News/Articles/Documents/Implementation_ePrivacy_Directive-Apr2012.pdf.
[3] http://tnij.org/quhi.
[4] http://tnij.org/quhj.
[5] http://tnij.org/qr2u.

Niezależnie od dyskusji nad zagadnieniami szczegółowymi zebranymi w bloku nr 1 ocenie poddano również tezy zawarte w „Raporcie dotyczącym retencji danych telekomunikacyjnych – propozycje wprowadzenia nowych regulacji ograniczających ingerencję organów państwowych w prywatność obywateli oraz wzmacniających mechanizmy kontroli nad służbami specjalnymi w kontekście prac nad zmianą przepisów dotyczących dostępu do danych telekomunikacyjnych" opracowanym w 2011 r. przez Ministra Jacka Cichockiego w charakterze Sekretarza Kolegium ds. Służb Specjalnych. Należy jednocześnie zaznaczyć, iż tezy te stanowią materiał wyjściowy dla opracowywanego w chwili obecnej projektu założeń ustawy o zmianie niektórych ustaw, w związku z pozyskiwaniem i wykorzystywaniem danych telekomunikacyjnych.

RETENCJA DANYCH

Uczestnicy uznali, że demokratyczne państwo powinno gwarantować obywatelom stosowny poziom ochrony i dysponować w tym celu odpowiednimi narzędziami. W ewoluującym środowisku technologicznym, chodzi nie tylko o poważne przestępstwa, ale i o uciążliwe dla obywateli i powszechne oszustwa internetowe. Z uwagi na proces i procedury pozyskania danych, a następnie ich przetwarzania przez uprawnione podmioty (policja, służby) umożliwiające identyfikację i ukaranie sprawcy, wg większości uczestników warsztatu uzasadnionym okresem jest 12 miesięcy. Swoje zastrzeżenia w tym zakresie zgłosiła Fundacja Panoptykon, która konsekwentnie twierdzi, że okres 6 miesięcy byłby wystarczający do zrealizowania celów obowiązkowej retencji danych. Skrócenie okresu retencji danych do 12 miesięcy przewiduje projekt nowelizacji ustawy Prawo telekomunikacyjne[6]. Jednocześnie należy wskazać, iż w Sejmie procedowany jest druk poselski Nr 306, który przewiduje skrócenie tego okresu do 6 miesięcy[7].

- Warto zaznaczyć, iż zmiany zaproponowane w projekcie nowelizacji ustawy Prawo telekomunikacyjne zostały ocenione jako „niewystarczające" w opinii Fundacji Panoptykon oraz GIODO[8].
- Uczestnicy spotkania zgodzili się – mimo różnych zastrzeżeń (w tym ogólnej krytyki obowiązku zatrzymywania danych telekomunikacyjnych ze strony Fundacji Panoptykon) – że akceptowalny byłby roczny okres retencji.

Uczestnicy podkreślili, że wdrożenie obowiązku retencji wynika z konieczności implementacji dyrektywy retencyjnej (2006/24/WE), która pozostawia państwom członkowskim swobodę jedynie w przedmiocie okresu retencji (od 6 do 24 miesięcy). Jednocześnie wszyscy uczestnicy mają świadomość, że w niektórych państwach członkowskich przepisy dotyczące retencji danych zostały zaskarżone jako niezgodne z konstytucją (Czechy, Węgry, Niemcy, Rumunia) lub pozostają nieimplementowane ze względów politycznych. W niektórych przypadkach wnioski uznane zostały za zasadne.

W Polsce, w sierpniu 2011 r. prof. Irena Lipowicz - Rzecznik Praw Obywatelskich - zaskarżyła do Trybunału Konstytucyjnego przepisy ustaw o policji, Straży Granicznej, kontroli skarbowej, Żandarmerii Wojskowej, Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, Centralnym Biurze Antykorupcyjnym, Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego oraz Służbie Celnej m.in. w zakresie udostępniania im danych telekomunikacyjnych. RPO zakwestionowała

[6] http://mac.bip.gov.pl/prawo-i-prace-legislacyjne/projekt-ust-z-dn-17-05-2012-o-zmianie-ust-prawo-telekomunikacyjne.html.
[7] http://tnij.org/qsid.
[8] http://m.onet.pl/biznes/5031339,detal.html.

m.in. to, że ustawy nie regulują precyzyjnie celu gromadzenia danych telekomunikacyjnych oraz nie nakazują służbom niszczenia tych, które okażą się nieprzydatne. Nie jest na dzień dzisiejszy znany termin sprawy przed Trybunałem Konstytucyjnym.

Zwrócono jednocześnie uwagę na fakt, iż dane podlegające retencji są przez przedsiębiorców telekomunikacyjnych również gromadzone dla innych celów min. rozliczeń i postępowania reklamacyjnego (na podstawie art. 168 ustawy Prawo telekomunikacyjne) – w ciągu roku od wykonania usługi klient ma prawo złożyć reklamację, dlatego przedsiębiorca musi mieć w tym czasie możliwość weryfikacji i ustosunkowania się do żądania wskazanego w reklamacji.

- ! Uczestnicy spotkania w większości zgodzili się, że retencja danych w demokratycznym państwie, którego jednym z celów jest zapewnienie obywatelom odpowiedniego poziomu bezpieczeństwa, jest w pewnym stopniu uzasadniona. Kwestią dyskusyjną pozostaje kształt retencji. Zastrzeżenia, analogiczne do cytowanych powyżej, wyrazili w tym zakresie przedstawiciele Fundacji Panoptykon.

KONTROLA

W opinii uczestników warsztatu istnieje realne ryzyko nadużywana przez podmioty uprawnione (w tym sądy i prokuratury) dostępu do i wykorzystywania danych retencyjnych, czego dowodzą statystyki dotyczące liczby zapytań o dane telekomunikacyjne w poszczególnych państwach członkowskich, cytowane w pkt. 5.1 sprawozdania Komisji dla Rady i Parlamentu Europejskiego z oceny dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE)[9]. W 2009 r. służby, policja i sądy sięgały do danych telekomunikacyjnych ponad milion razy. Zgodnie ze statystykami gromadzonymi przez Urząd Komunikacji Elektronicznej, w 2010 r. ta liczba zwiększyła się o ponad 1/3. W 2011 roku zrealizowano ponad 1,85 milionów zapytań[10]. Z tego powodu niezbędne jest wprowadzenie pewnych mechanizmów przeciwdziałających.

Proponowana przez MSW instytucja pełnomocnika działającego w ramach każdej ze służb nie jest wystarczająca, rozwiązanie ocenione zostało przez uczestników jako „listek figowy". Organ kontrolny powinien być jeden oraz powinien być organem zewnętrznym w stosunku do podmiotów uprawnionych – naturalnym organem powinien być zatem Generalny Inspektor Ochrony Danych Osobowych.

W trakcie dyskusji pojawiły się również postulaty, że należy sformalizować procedurę sięgania po dane poprzez wprowadzenie jasnych procedur (np. na wzór brytyjski, gdzie przy sięganiu po dane funkcjonariusz wypełnia formularz wskazując, w jakim celu potrzebne są dane, jak pomogą w sprawie, jakie jest źródło informacji o telefonie i dlaczego nie da się sprawy rozwikłać bez odwołania do tych danych).

- ! Uczestnicy spotkania zastrzegli, że sposób wykorzystywania danych powinien być poddany zewnętrznej w stosunku do służb kontroli, a obywatele powinni mieć zagwarantowane prawo do informacji o tym, czy ich dane były przedmiotem kontroli (poza precyzyjnie wyliczonymi przypadkami, np. ze względu na bezpieczeństwo państwa).

[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:PL:PDF.

[10] http://www.panoptykon.org/wiadomosc/ile-razy-panstwo-siegalo-po-nasze-dane-telekomunikacyjne-w-2011-roku-publikujemy-najnowsze.

OBOWIĄZKI STATYSTYCZNE

Uczestnicy warsztatu byli zgodni co do tego, że obecne informacje w zakresie statystyk są zdecydowanie niewystarczające - statystyki powinny być ogólnie dostępne, bardziej szczegółowe i gromadzone również przez służby, prokuraturę i sądy.

Dyskusyjna jednak jest kwestia, co dokładnie powinno być przedmiotem statystyk – zgodzono się, że obywatele powinni mieć dostęp w szczególności do informacji o:

- liczbie numerów (telefonicznych, IP), w stosunku do których wystąpiono z zapytaniem,
- liczbie spraw, których takie zapytanie dotyczyło,
- rodzaju zapytania (w związku z naruszeniem jakich przepisów) oraz
- okresie (jak daleko wstecz) pozyskania danych.

W trakcie dyskusji pojawiła się również koncepcja budowy systemu teleinformatycznego wspólnego dla służb lub w ramach poszczególnych służb, do którego wprowadzano by dane dotyczące poszczególnych zapytań. Z jednej strony system okazałby się niezwykle pomocny na potrzeby generowania statystyk, z drugiej natomiast eliminował przypadki wielokrotnego zapytywania o ten sam numer przez np. poszczególne komendy policji.

INFORMOWANIE OBYWATELI

Uczestnicy warsztatu zwrócili uwagę na fakt, iż po zakończeniu sprawy lub postępowania obywatele powinni otrzymywać informację, że dane ich dotyczące były zbierane i przetwarzane na potrzeby postępowań. Spod takiego obowiązku wyłączone powinny być jednak sprawy związane z bezpieczeństwem państwa. Wyłączenie powinno być przedmiotowe (sprawy), a nie podmiotowe (całe służby).

WPROWADZENIE ODPŁATNOŚCI ZA DANE UDOSTĘPNIANE SŁUŻBOM

Uczestnicy warsztatu poddali pod dyskusję kwestię wprowadzenia odpłatności za pozyskiwanie danych przez podmioty uprawnione. Z doświadczenia usługodawców działających na podstawie ustawy o świadczeniu usług drogą elektroniczną, którzy taka odpłatność wprowadzili, wynika, że jest to skuteczne narzędzie wymiernie ograniczające pozyskiwanie danych retencyjnych.

Zwrócono również uwagę na fakt, że przedsiębiorcy telekomunikacyjni ponoszą realne koszty związane z retencją. Koszty związane są głównie nie z realizacją obowiązku zachowywania danych, ale z procedurą ich udostępniania, zatem nawet po skróceniu okresu retencji z dwóch lat – jak obecnie – do roku czy do 6 miesięcy koszty te dalej będą generowane. Podkreślono, że sądy i prokuratura płacą dostawcom usług świadczonych drogą elektroniczną (których obowiązek retencyjny nie dotyczy) za przekazywane dane, zatem obciążenia nałożone na przedsiębiorców telekomunikacyjnych są z nieuzasadnionych przyczyn większe i nieproporcjonalne.

GWARANCJE OCHRONY TAJEMNICY ZAWODOWEJ

Uczestnicy poruszyli problem tajemnic zawodowych, które są niejednokrotnie naruszane przy wykorzystaniu przepisów dotyczących retencji. Zaproponowano postulat adresowany do Ministra Sprawiedliwości, aby dane o lokalizacji, bilingi i inne, które mogą posłużyć np. do identyfikacji informatora, objąć szczególną procedurą dotyczącą ochrony tajemnicy zawodowej. W modelu opartym na kontroli dostępu do danych telekomunikacyjnych przez sąd lub prokuratora, organ kontrolny powinien być informowany o szczególnym statusie konkretnych danych, jeśli jest to informacja znana na etapie składania wniosku o dane. Również w przypadku identyfikacji materiałów objętych tajemnicą zawodową, takie materiały powinny być usuwane z akt sprawy.

KONKLUZJE I REKOMENDACJE

1. Zasadne jest ograniczenie okresu retencji danych do jednego roku (z obecnie obowiązujących dwóch lat). Wspomniane powyżej zastrzeżenie zgłosiła w tym zakresie Fundacja Panoptykon.
2. Większość zmian procedowanych na podstawie „Raportu dotyczącego retencji danych telekomunikacyjnych – propozycje wprowadzenia nowych regulacji ograniczających ingerencję organów państwowych w prywatność obywateli oraz wzmacniających mechanizmy kontroli nad służbami specjalnymi w kontekście prac nad zmianą przepisów dotyczących dostępu do danych telekomunikacyjnych" w praktyce nie przyczyni się do ograniczenia dostępu do i wykorzystywania danych zachowywanych przez przedsiębiorców telekomunikacyjnych („listek figowy") i co do zasady – należy się do nich odnieść krytycznie;
3. Powoływanie w ramach każdego podmiotu instytucji pełnomocnika nie może być uznane za rozwiązanie wystarczające z perspektywy zapewnienia odpowiedniej kontroli i nie ograniczy dostępu do i wykorzystywania danych.
4. Realne ograniczenie w przypadku pozyskiwania danych stanowić będzie wprowadzenie obowiązku odpłatności za ich pozyskanie.
5. Organ kontrolny powinien mieć charakter zewnętrzny w stosunku do podmiotów uprawnionych.
6. Niezbędne jest opracowanie przejrzystych procedur wnioskowania o dostęp do danych.
7. Pojawił się postulat utworzenia bazy danych o wnioskach o dostęp do danych retencyjnych i o ich przetwarzaniu – w takiej sytuacji każdy z podmiotów przed wnioskowaniem o dostęp mógłby sprawdzić w bazie, czy dane, które zamierza pozyskać, nie zostały już przez ten sam podmiot pozyskane.
8. Niezbędne jest wprowadzenie obowiązku sprawozdawczego dotyczącego statystyk pozyskiwania danych retencyjnych (dla potrzeb statystyk zastosowanie znajdzie wspomniana wyżej baza danych).
9. Obywatele powinni być informowani o fakcie pozyskania i wykorzystania danych ich dotyczących (po zakończeniu postępowania). Wyjątki powinny dotyczyć spraw związanych z bezpieczeństwem państwa.
10. Tajemnice zawodowe powinny podlegać szczególnej ochronie i konieczne jest wprowadzenie konkretnych mechanizmów, które tę kontrolę zapewnią;
11. Wskazanie w umowie parametrów usługi (dostępu do sieci Internet) będzie się wiązać z koniecznością zachowywania i przetwarzana danych o usłudze. Alternatywnym rozwiązaniem byłoby zobowiązanie operatora do badania łączy w odpowiednich interwałach (testy operatora).

Trzecie spotkanie – bloki tematyczne Nr 3 i 4
Monitoring aktywności w sieci telekomunikacyjnej

Dyskusja skupiła się na problemie możliwości podejmowania przez przedsiębiorców telekomunikacyjnych działań zmierzających do eliminacji komunikatów, które mogą stanowić zagrożenie dla sieci lub usług oraz zmierzających do ograniczenia lub przerwania świadczenia usługi z tego samego powodu. Dyskutowano również o potencjalnej możliwości nadużywania tego przepisu przez przedsiębiorców.

Zebrani uznali, że obecnie stosowane procedury reklamacji są wystarczające dla abonentów, w przypadku usuwania komunikatów stanowiących zagrożenie dla bezpieczeństwa sieci lub usług oraz w przypadkach ograniczenia lub przerwania usługi.

Przedstawiciele dostawców usług podkreślali, że warto doprecyzować przepisy na wypadek sytuacji, gdy ruch dostawcy treści jest w sieci przez operatora ograniczany (degradowany). Operatorzy zauważyli, że wystarczą w tym zakresie procedury reklamacyjne i komunikacja z UKE. Gdyby np. zmusić operatorów do ujawnienia, jak duży ruch są w stanie utrzymać bez „przycinania", byłoby to zaproszeniem do ataków DDOS. Poza tym „przycinanie" ruchu – po to, by zachować jego płynność – zdarza się nieustannie, jest generowane automatycznie, w związku z czym raporty w tej sprawie byłyby ogromnym i nieuzasadnionym przeciążeniem informacyjnym.

W przypadku blokowania „na końcówce" – kiedy np. użytkownik jest odcinany z powodu treści, które wrzuca do sieci (zagrażającej bezpieczeństwu sieci lub usług), poprzedzone to jest tyloma ostrzeżeniami, że dodatkowe raporty lub informacje na stronach internetowych, nie mają uzasadnienia. Natomiast użytkownik w przypadku odcięcia od Internetu i tak zadzwoni do operatora, by dowiedzieć się o przyczynę.

W trakcie dyskusji poruszono również kwestię wymieniania się przez przedsiębiorców telekomunikacyjnych informacjami na temat zagrożeń, również potencjalnie zawierającymi dane o użytkownikach lub przekazywanych treściach. Ustalono, że przedsiębiorcy wymieniają się adresami IP i fragmentarycznymi danymi o komunikatach (nagłówki IP) wskazujących na rodzaj zagrożenia dla sieci, ale nie pozwala to na identyfikowanie konkretnych osób.

W świetle powyższego ze strony dostawców treści padł postulat poszerzenia listy podmiotów, które mogą wymieniać się takimi informacjami (o usługodawców w rozumieniu ustawy o świadczeniu usług drogą elektroniczną).

KONKLUZJE I REKOMENDACJE

1. Przedsiębiorcom telekomunikacyjnym powinno przysługiwać omawiane uprawnienie, w celu ochrony sieci, usług i samych użytkowników.
2. Nie jest zasadne konkretyzowanie przesłanek podejmowania tego typu działań przez przedsiębiorcę, z uwagi na niezwykle szybko ewoluujące technologie. Przedsiębiorca powinien być w stanie dobierać środki odpowiednie do zidentyfikowanego zagrożenia.
3. Co do zasady – nie ma zagrożenia nadużywania przez przedsiębiorców przepisu. Obowiązani są oni bowiem informować Prezesa UKE o podjętych działaniach. Prezes UKE będzie mógł w drodze decyzji zakazać stosowania przyjętego przez przedsiębiorcę rozwiązania.
4. Dostawcy treści powinni być informowani o ograniczaniu ich ruchu.
5. Nie ma konieczności wprowadzania obowiązku informacyjnego dla użytkownika, który w przypadku ograniczenia lub przerwania usługi może złożyć do przedsiębiorcy reklamację. Jednocześnie, realizacja takiego obowiązku natrafiałaby na poważne problemy logistyczne (w przypadku odcięcia użytkownika od sieci informacja musiałaby docierać innym kanałem) i generowałaby koszty, które w praktyce byłyby przerzucane na użytkowników końcowych. Natomiast w praktyce – przedsiębiorca przed wprowadzeniem ograniczenia lub przerwaniem usługi wielokrotnie kontaktuje się z abonentem.

6. Pojawił się postulat dotyczący uwzględnienia w brzmieniu art. 175c ust. 5 usługodawców w rozumieniu ustawy o świadczeniu usług drogą elektroniczną – zdania co do jego uwzględnienia są podzielone.
7. Wymiana adresów IP między przedsiębiorcami telekomunikacyjnymi w celu przeciwdziałania zagrożeniom w sieci telekomunikacyjnej stanowi uzasadniony przypadek przetwarzania danych mający oparcie w przepisach prawa, a zatem sankcjonowany przez ustawę o ochronie danych osobowych.

Blokowanie treści

W tym punkcie dyskutowano nad możliwością wprowadzenia obowiązku blokowania dostępu w sieci Internet do treści pedofilskich (a nie ich usuwania z serwerów), który spoczywałby na operatorach telekomunikacyjnych.

Wszyscy byli zgodni co do tego, że z problemem pedofilii należy bezwzględnie walczyć. Jednak, choć wdrażana dyrektywa unijna umożliwia wprowadzenie w prawach narodowych państw członkowskich obowiązku blokowania dostępu do tego typu treści, uznano, że rozwiązanie to jest nieefektywne, drogie, nieskuteczne i szkodliwe z punktu widzenia wartości chronionych w demokratycznym państwie prawa. Co więcej, nie pozwala „namierzać" pedofilów w momencie, kiedy uzyskują dostęp do takich treści lub sami je generują i wprowadzają do sieci.

W trakcie dyskusji przywołano fakt opracowania rekomendacji zespołu zadaniowego Komitetu Rady Ministrów Informatyzacji i Łączności ds. zmian do ustawy Prawo telekomunikacyjne zamieszczonych w projekcie ustawy o zmianie ustawy o grach hazardowych oraz niektórych innych ustaw (Rejestr Stron i Usług Niedozwolonych)[11] obradującego pod koniec 2009 r. Uznano te rekomendacje za aktualne również w tym przypadku.

Uznano, że niezbędne jest zwiększenie efektywności usuwania tego typu treści, w związku z niską skutecznością i wysoką społeczną szkodliwością ewentualnego blokowania do nich dostępu.

KONKLUZJE I REKOMENDACJE

1. Blokowanie dostępu do treści pedofilskich jest nieskuteczne, nieopłacalne i nieefektywne. Podejmowanie takich prób jest z góry skazane na niepowodzenie.
2. Wdrożenie do polskiego porządku prawnego przepisu dyrektywy spowoduje, że operatorzy w celu klasyfikacji treści musieliby się z nią zapoznawać, czego robić im nie wolno.
3. Wdrożenie takiego rozwiązania doprowadzi do przypadków naruszania praw innych podmiotów w wyniku blokowania również treści legalnych.
4. Blokowanie takich treści uniemożliwi identyfikację pedofilów i podjęcie stosownych działań;
5. Niezbędne jest zwiększenie efektywności usuwania takich materiałów z sieci, identyfikacji i karania pedofilów.

[11] http://krmc.mac.gov.pl/download/50/1695/Rekomendacje.pdf.

Podsumowanie

Przeważają opinie, by kontynuować prace zespołu w formacie taskforce – to unikalne miejsce na dyskutowanie o szczegółach rozwiązań po to, by się nawzajem zrozumieć. Pojawiają się również opinie negatywne, szczególnie ze strony organizacji pozarządowych, które przed ewentualną kontynuacją prac postulują przemyślenie celów i metod działania.