Ochrona danych osobowych – teoria i fikcja

Krzysztof Billewicz

W dzisiejszych czasach w Europie bardzo dużą uwagę zwraca się na ochronę danych osobowych, które można przypisać do konkretnej osoby fizycznej. Oprócz tego – w wyniku obowiązywania Ustawy o ochronie danych osobowych obywatelom ogranicza się dostęp do danych osobowych innych obywateli, nawet gdy dany człowiek stanie się ofiarą wykroczenia lub przestępstwa. Do niektórych danych dostęp mają jedynie organy ścigania (oczywiście również organy skarbowe), do innych dostęp taki musi umożliwić wyrok sądowy, np. uchylenie tajemnicy bankowej.

Takie postępowanie byłoby słuszne, gdyby tuż obok nie funkcjonowaliby globalni giganci internetowi, którzy bez problemu mają dostęp do bardziej poważnych danych, dotyczących setek milionów klientów, czy wręcz do danych wrażliwych na temat klientów. Tacy klienci nie tylko nie wiedzą, jakie przedsiębiorstwo IT przetwarza dane osobowe na ich temat, nie mają żadnego dostępu do tych danych ani nie mogą cofnąć zgody (której zresztą nie udzielili) na temat przetwarzania takich danych. Na przykład firma dostarczająca przeglądarkę internetową może przechowywać historię zapytań dla danego IP komputera danego konta (jeżeli klient zalogował się) lub dla danego adresu e-mail. Co więcej, doświadczenie pokazuje, że jeżeli jakaś informacja znajdzie się w Internecie, to jej całkowite usunięcie po pewnym czasie staje się zupełnie niemożliwe. Nie ma możliwości określenia, gdzie jeszcze jest przechowywana kopia tej informacji.

Przeciętny obywatel wie, że niektórzy globalni giganci internetowi przetwarzają ogromne ilości danych na jego temat, z drugiej strony nie może uzyskać wiedzy na ten temat ani zabronić przetwarzania takich danych. Okazuje się, że dla przeciętnego klienta ustawa ta ogranicza prawa dostępu do danych osobowych dotyczących innych osób, natomiast w żaden sposób nie ma zastosowania do globalnych gigantów internetowych, przetwarzających dane osobowe tego klienta. Firmy te mają siedziby w różnych krajach, dlatego też ustawodawstwo krajowe może ich zupełnie nie dotyczyć.

Dane osobowe – teoria

Ust. 6 ustawy o ochronie danych osobowych, który stanowi, że:
– dane osobowe są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Określenie – wszelkie informacje – oznacza jakiekolwiek dane dotyczące określonej osoby, a więc zarówno dotyczące: jej życia zawodowego, prywatnego, stosunków majątkowych, grupy krwi czy też cech charakteru. Będą nimi zarówno aspekty językowe i pozajęzykowe, a więc nie tylko: imię, nazwisko, PESEL, adres, ale też linie papilarne lub wygląd,
– osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, zwłaszcza przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne,
– informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Danymi osobowymi zatem będzie każda informacja, która pozwala na zidentyfikowanie osoby nawet pośrednio przy uwzględnieniu innych informacji, chyba że wymagałoby to nadmiernych kosztów, czasu lub działań. Danymi osobowymi zatem jest: adres IP komputera, zdjęcie, adres e-mail (zwłaszcza jeśli składa się z imienia i nazwiska), jeżeli za ich pomocą będzie możliwa identyfikacja konkretnej osoby.

Dane wrażliwe to szczególny (sensytywny) rodzaj danych osobowych. Zgodnie z 27 ust. 1 Ustawy o ochronie danych osobowych, danymi wrażliwymi są informacje z zamkniętej listy:
– o pochodzeniu rasowym lub etnicznym,
– poglądach politycznych, przekonaniach religijnych lub filozoficznych,
– przynależności wyznaniowej, partyjnej lub związkowej,
– stanie zdrowia,
– kodzie genetycznym,
– nałogach,
– życiu seksualnym,
– dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzanie danych wrażliwych jest poddane szczególnemu trybowi. Istnieje generalny zakaz przetwarzania tych danych z wyjątkiem sytuacji, na które zezwalają przepisy prawa. W świetle wcześniej przedstawionej definicji danych osobowych należy założyć, że danymi osobowymi nie będą pojedyncze informacje o dużym stopniu ogólności, np. nazwa ulicy i numer domu czy wysokość wynagrodzenia. Informacja taka stanie się jednak danymi osobowymi wówczas, gdy zostanie zestawiona z innymi dodatkowymi informacjami, które w konsekwencji można odnieść do konkretnej osoby [4].

W art. 6 Ustawy o ochronie danych osobowych ustawodawca posłużył się klauzulą generalną. Nie określił zatem zamkniętego katalogu informacji, które stanowią dane osobowe. W konsekwencji takiego podejścia, przy rozstrzyganiu czy określona informacja lub informacje stanowią dane osobowe, w większości przypadków nieuniknione jest dokonanie zindywidualizowanej oceny, przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby [4].

W USA główny akcent stawia się na ochronę prywatności, która jest bardzo ceniona przez obywateli, zaś w Europie na ochronę danych osobowych.

Zagrożenia prywatności

Można wyobrazić sobie sytuację, że na rynku pojawia się nowa firma oferująca usługi pocztowe. Swoje usługi będzie reklamować

Dr inż. Krzysztof Billewicz – Instytut Energoelektryki Politechniki Wrocławskiej (krzysztof.billewicz@pwr.edu.pl)

jako darmowe, zachęcając do wysyłania jak największej liczby listów i podkreślając, że to nie do pomyślenia, aby w XXI w. ludzie jeszcze płacili tak dużo za znaczki pocztowe i nadanie listu. Z usług tej nowej firmy można będzie korzystać bez pieniędzy i bez karty bankowej. Kiedy jednak wczytamy się w regulamin świadczenia usługi – okazuje się, że gdzieś pod koniec – małymi literami jest zapisana formuła zgody na czytanie i zapamiętywanie treści naszych listów na serwerach tej nowej firmy, a także na dołączanie reklam [1]. Dodatkowo firma pocztowa będzie interesowała się tym, o czym piszemy, w jaki sposób i do kogo. Na tej podstawie zgromadzi na nasz temat sporą wiedzę, na podstawie której do koperty będzie wkładać reklamy. Oczywiście będzie to „darmowa" usługa pocztowa, jedynie za cenę naszych danych osobowych, prywatności i zgody na pośredniczenie w reklamowaniu produktów. Pojawia się zatem pytanie – czy taka usługa rzeczywiście jest darmowa [1]?

Nie jest to fikcją czy daleką przyszłością. Już teraz w taki sposób funkcjonuje wiele przedsiębiorstw. Najczęściej internauta jest przekonywany lub nawet zmuszany przez dostawców darmowych usług cyfrowych do rezygnacji ze swojej prywatności. Taki model biznesowy funkcjonuje tym lepiej, im trafniej przewidzi się podatność internauty na argumenty za zakupieniem określonego produktu lub usługi [1]. Niektóre portale społecznościowe i bardzo wiele aplikacji na smartfony funkcjonuje na tych zasadach. Klienci jednak cieszą się, że mogą za darmo z korzystać z takich usług. Można powiedzieć, że gdyby ten model biznesowy nie przynosił oczekiwanych zysków twórcom takiego oprogramowania lub takich usług, to tego typu rozwiązania nie byłyby dostępne.

Obecnie wiedza zdobyta na podstawie prywatnych e-maili, wiadomości sms, czy wymienianych na komunikatorze internetowym na podstawie wyszukiwanych haseł w przeglądarce, jest przetwarzana nie tylko na komunikaty „kup to", „musisz to mieć", „promocja", „wyprzedaż", ale również pozwala poznać nasze słabe strony, choroby, podatność na określoną retorykę (strachu, korzyści itp.). Wiele osób poszukuje określonych usług jedynie w Internecie. W zasadzie nie rusza się spoza komputera. Dlatego też na podstawie pozyskanej wiedzy o słabościach klienta generowane są założenia: zaoferowania droższej polisy ubezpieczeniowej, nie udzielania rabatu, ponieważ nie ma on innego wyjścia, jak tylko skorzystać z tej usługi [1]. Zatem za świadczoną usługę – np. korzystanie z „darmowego" oprogramowania – klient po prostu zapłaci za reklamowane produkty albo wręcz będzie zmuszony do tego przez oferowanie mu zawyżonych cen pewnych usług.

Firmy wiedzą, że dzięki naruszeniu prywatności internautów mogą świadczyć im dodatkowe usługi, czy wręcz pomagać im (i oczywiście reklamodawcom, którzy zapłacili najwięcej). Dlatego reklamy są dostosowywane do konkretnego klienta, jego zainteresowań i oczekiwań. Pisząc w wiadomości o planowanych wakacjach i chęci pojechania do Egiptu pojawi się reklama biura podróży oferującego taką usługę. Podobnie poszukując mieszkania do zakupu – pojawi się reklama deweloperów oferujących właśnie takie mieszkania.

Połączenie ze sobą przetwarzania wielkich zbiorów danych, w tym zbieranie i zestawianie danych z wielu źródeł, wykorzystania chmury obliczeniowej, urządzeń mobilnych i personalizacji to największe obecnie zagrożenia dla prywatności. Przykładem ujawniania bez zgody osób, których te dane dotyczą i wykorzystania takich danych jest program PRISM. Jest on jednym z najważniejszych źródeł danych udostępnianych dobrowolnie przez amerykańskich gigantów internetowych dla amerykańskich agencji zajmujących się bezpieczeństwem, które mają stały, pełny i niekontrolowany dostęp do danych przechowywanych na serwerach tych wielkich firm.

Obecnie obserwuje się dwie postawy związane z ochroną prywatności:

– dyktat i przewrażliwienie na tym punkcie instytucji publicznych,
– dwuznaczną postawę części społeczeństwa, które z jednej strony chciałoby chronić swoją prywatność, dane osobowe i wykazywać wielką wrażliwość na możliwe wykorzystanie danych z inteligentnych liczników jako danych mówiących o prywatności. Jednak z drugiej strony masowo zrzekają się oni prywatności i udostępniają swoje prywatne informacje, aby móc za darmo korzystać z części usług internetowych, gier i programów komputerowych.

W wyniku takiego podejścia okazuje się, że bardzo wiele globalnych firm przechowuje i przetwarza dane osobowe, w tym również dane wrażliwe o osobach, treść ich korespondencji, listę odwiedzanych witryn stron www, informacje o hasłach wpisywanych w wyszukiwarkach. Dzięki zapamiętywaniu prywatnych danych internetowe narzędzia dostosowują się do konkretnego klienta – personalizują się. Z jednej strony jest to korzystne dla klienta, z drugiej natomiast oddanie prywatności jest ceną za korzystanie z „darmowych" usług.

Tak zgromadzone dane i informacje są wykorzystane do dobierania i wyświetlania spersonalizowanej reklamy skierowanej do klienta. Mogą również być one wykorzystane przez bank, towarzystwo ubezpieczeniowe, a nawet przez służby wywiadowcze. Zatem za darmowe usługi „płaci się", udostępniając dane osobowe i zezwalając na ich przetwarzanie. W konsekwencji ceną jest prywatność i w pewnym zakresie również społeczna wolność.

Giganci internetowi mają dane kwalifikowane swoich klientów i są one traktowane jako dane wrażliwe: o ich chorobach (w tym zaburzeniach psychicznych), światopoglądzie, wyznawanej religii, preferencjach seksualnych, wadach. Czasami również mogą mieć i przechowywać dane, których ujawnienie może być kompromitujące dla danej osoby: dane o wykroczeniach lub nawet o przestępstwach, które dana osoba planowała, widziała, na które przyzwoliła lub w których uczestniczyła. Nasuwa się oczywiste pytanie, jeżeli takie dane są przechowywane, to również mogą zostać sprzedane – mają określoną wartość na rynku, mogą przyczyniać się do świadczenia dodatkowych „usług" na rzecz klientów. Jeżeli zatem jakiś podmiot może na nich dużo zarobić, to ich wykorzystanie do celów zarobkowych wydaje się być jedynie kwestią czasu.

Osoby, których te dane dotyczą, nie mają żadnej możliwości domagania się wglądu, uaktualnienia lub bezpowrotnego usunięcia takich danych ze wszystkich miejsc, gdzie takie dane są przechowywane. Przechowywana jest również historia aktywności na portalach społecznościowych, sieć znajomych, dane osobowe, w tym poglądy polityczne, światopogląd itp. Dlatego akcentowanie w Europie ochrony danych osobowych powinno skutkować również prawem do dostępu, wglądu do kompletu danych zgromadzonych na swój temat przez globalnych gigantów internetowych oraz prawa do cofnięcia zgody na ich przechowywanie i przetwarzanie oraz gwarancji bezpowrotnego usunięcia takich danych.

Przykładowo niektórzy giganci internetowi bronią się, że przetwarzają i przechowują dane, które i tak są publicznie dostępne dla wszystkich w Internecie. Giganci argumentują, że nie kontrolują tych danych, tylko udostępniają linki do informacji, które ktoś inny

zamieścił w Internecie. W takim przypadku klienci zostają pozbawieni „prawa do bycia zapomnianym" (right to be forgotten). Jest to prawo osób prywatnych do wykreślenia z obiegu publicznego informacji dotyczących samych zainteresowanych.

W zakresie ochrony prywatności również trzeba zauważyć, że w ramach różnych programów (zbieranie punktów w supermarkecie) lub aplikacji na smartfony czy komputery (np. lista zakupów) można zebrać zbiorcze fragmenty danych, które odnoszą się do ich usług przyporządkowanych do jednej osoby. W ten sposób można dokonać odkrycia pewnych cech osobowych, zwłaszcza tzw. danych wrażliwych, np. na podstawie regularnie kupowanych rodzajów żywności można ujawnić wyznawaną religię lub występujące problemy zdrowotne, czy wręcz choroby przewlekłe. Zgromadzone informacje o kupowanej prasie codziennej mogą świadczyć o wyznawanej religii, poglądach politycznych, cechach charakteru, preferencjach seksualnych. Zapewnienie bezpieczeństwa takich danych staje się poważnym wyzwaniem.

Uderza nie tylko to, że dane osobowe są dostępne i przechowywane, ale również to, że są one zgromadzone w jednym miejscu (bardzo szybko i łatwo dostępne) oraz to, że mogą być one wykorzystywane bez wiedzy i zgody osoby, której one dotyczą.

W dzisiejszej sytuacji problem ochrony jest bardzo złożony. Niemal każdy człowiek ma przy sobie telefon komórkowy. Operator sieci komórkowej ma zatem informacje o tym, gdzie właśnie znajduje się dana osoba, z kim się spotyka. Aby mieć takie informacje – wcale nie trzeba nikogo śledzić.

Przed zainstalowaniem niektórych aplikacji na smartfony użytkownik jest informowany, do jakich danych aplikacja będzie miała dostęp. Mogą to być prywatne pliki przechowywane w telefonie, a nawet lista osób znajomych i dostęp do treści prywatnych wiadomości sms. Duża część użytkowników nie czyta takich informacji, tylko domyślnie je akceptuje. Aplikacja może wysłać niektóre z tych informacji na serwery za pośrednictwem sieci. Konieczne jest uczulanie użytkowników, którzy mają służbowe smartfony przed instalowaniem takich aplikacji. Podobnie zresztą duża część użytkowników nie czyta regulaminów świadczenia usług lub zasad obowiązywania licencji nowo instalowanego oprogramowania komputerowego. Domyślnie akceptują takie zapisy.

Głos klienta

Wiele danych dotyczących klienta może zostać zdobytych i wykorzystanych bez jego wiedzy i zgody. Przykładowo wiele firm świadczy usługi za pośrednictwem telefonu. W takim przypadku (…) *w trosce o bezpieczeństwo i najwyższą jakość świadczonych usług* (…) rozmowa z klientem jest nagrywana. Klient, aby skorzystać z takiego kanału komunikacyjnego musi wyrazić zgodę na nagrywanie. Taki klient nie wie, jakie jego dane osobowe będą wykorzystywane przez przedsiębiorstwo i w jaki sposób. Taka nagrana rozmowa jest ewentualnym dowodem w przypadku sporu pomiędzy klientem a usługodawcą. Jednak znane są możliwości analizy głosu klienta. Na jego podstawie można określić pewne cechy klienta, które później mogą być wykorzystane zarówno do odpowiedniego doboru rozmówcy do danego klienta, jak również do sposobu prowadzenia takiej rozmowy i do doboru produktów jemu oferowanych. Najczęściej głos klienta (VoC – voice of the customer) może dotyczyć rozpoznania odpowiedniego podejścia (oczekiwań, preferencji i niechęci) klienta i dzięki temu przygotowanie się usługodawcy do spełniania oczekiwań oraz zaspokajania potrzeb. VoC to połączenie konkretnego klienta z przedsiębiorstwem. To informacja zwrotna o jakości świadczonych usług. Analiza głosu może być zarówno jakościowa jak i ilościowa.

Na podstawie analizy głosowej takiej rozmowy można jednak uzyskać dużo więcej informacji, od podstawowych cech temperamentu: choleryk/flegmatyk, kompetentny/problemowy – do takich, jak: warto lub nie watro utrzymywać z nim kontaktu, warto lub nie dostosować ofertę do tego klienta i zastosować zniżki, upusty, bonifikaty. Na podstawie głosu klienta można przypisać klienta do odpowiedniego segmentu, można przygotować odpowiednie pytania i przewodnik do prowadzenia dyskusji oraz na podstawie obserwacji i analizy wywiadów sposobów wydobywania z klienta określonych informacji. Dzięki zastosowaniu odpowiednich narzędzi socjologiczno-psychologicznych możliwe staje się precyzyjne wyjaśnienie kluczowego pytania stawianego w każdym realizowanym projekcie – czego wymaga/oczekuje klient?

Problematyka prywatności w inteligentnych systemach pomiarowych

Niejako w przeddzień wdrażania inteligentnych liczników na masową skalę zwraca się uwagę na ryzyko ujawnienia danych pomiarowych, które mogą opisywać nawyki i zwyczaje poszczególnych odbiorców końcowych energii elektrycznej. W przypadku danych pomiarowych może być to o tyle dyskusyjne, że np. na zużycie energii przez gospodarstwo domowe składa się zsumowany pobór przez wszystkich mieszkańców (i gości). Jednak nawet jeżeli 1% danych można przywiązać do konkretnej osoby, to wtedy są to dane osobowe. Przykładowo, jeżeli przez tydzień występuje zerowy pobór energii, to można wprost powiedzieć, że żaden z mieszkańców nie pobiera żadnej energii. Generalny Inspektor Ochrony Danych Osobowych stoi na straży ochrony przewidzianej w Ustawie o ochronie danych osobowych – dane pomiarowe o zużyciu energii są danymi osobowymi.

Oczywiście ciekawe byłoby, czy również np. współczynnik odkształcenia harmonicznymi napięcia zasilającego *THD* jest rodzajem danych osobowych. Parametr *THD* określa poziom zniekształceń sinusoidy napięcia, a deformacja kształtu sinusoidy napięcia może być wynikiem nieliniowego charakteru poboru prądu przez wykorzystywane odbiorniki energii elektrycznej, takie jak urządzenia energoelektroniczne (np. zasilacze UPS, falowniki) lub urządzenia wyposażone w coraz powszechniej stosowane zasilacze impulsowe (telefony komórkowe, sprzęt informatyczny). Współczynnik ten może mówić o odbiornikach wykorzystywanych przez klienta końcowego, czyli może mówić o pewnych nawykach lub zwyczajach.

Inteligentne systemy pomiarowe muszą być zabezpieczone przed próbami kradzieży tożsamości odbiorcy oraz przed nieautoryzowanym dostępem. Dodatkowo pracownicy przedsiębiorstwa dystrybucyjnego lub pracownicy dostawcy oprogramowania mogą chcieć użyć danych osobowych odbiorców do celów innych niż realizacja i rozliczanie dostaw energii, zarządzanie popytem, czy nadzorowanie dokonywanych płatności. Należałoby w pewien sposób ograniczyć możliwość wykorzystania danych osobowych, gromadzonych w bazach w systemach informatycznych w przedsiębiorstwach elektroenergetycznych do celów niezwiązanych z realizacją misji konkretnego przedsiębiorstwa – czyli wykorzystania ich w innym celu niż prawidłowe rozliczanie świadczonej usługi dostawy energii elektrycznej [3].

Niektórych odbiorców niepokoi brak kontroli nad gromadzeniem, przetwarzaniem, dostępem oraz wykorzystywaniem wrażliwych danych osobowych. Problem oczywiście jest nieco szerszy i dotyczy również nieautoryzowanego gromadzenia, pozyskiwania, wykorzystywania i ujawniania innych informacji. Dlatego też potrzebna jest kompleksowa strategia na rzecz ochrony prywatności w Internecie, najlepiej jako część narodowej strategii dostępu do szerokopasmowego Internetu [3]. Okazuje się bowiem, że osoby trzecie mogą gromadzić dane personalne i wykorzystywać do własnych celów. Uważa się, że taki ogromy zbiór danych osobowych, zawierający informacje o milionach odbiorców energii może być zarówno niebezpieczny jak i wykorzystany niezgodnie z przeznaczeniem.

Inteligentne sieci oraz systemy pomiarowe, które jednoznacznie identyfikują poszczególne urządzenia i ich zastosowanie, stwarzają nowe zagrożenia dla prywatności i mogą ujawniać intymne szczegóły życia rodzinnego.

Istnieje prawdopodobieństwo znaczącego zaangażowania osób trzecich lub przedsiębiorstw usług energetycznych w realizację i wsparcie wdrażania inteligentnego pomiaru. Stopień zaangażowania i wpływu osób trzecich będzie różnił się w zależności od państwa członkowskiego, ale oczywiste jest, że wdrożenie inteligentnego pomiaru – w jego najbardziej inwazyjnej postaci – może prowadzić do handlu profilami energetycznymi w interesie stron chcących sprzedawać usługi energetyczne. Im bardziej przetwarzanie ingeruje w prywatność, tym bardziej rygorystyczne muszą być środki ochronne [2].

U podstaw wszystkich tych środków leżałaby zgoda konsumenta, przy czym branża musiałaby zapewnić osobie (której te dane dotyczą) możliwość udzielenia takiej zgody w świadomy sposób. Niemożliwa do zaakceptowania z prawnego punktu widzenia byłaby sytuacja, w której osoby trzecie przetwarzałyby szczegółowe informacje na temat użytkowania energii przez osobę, której dane dotyczą, bez jej wiedzy i zgody [2].

Kwestie dyskusyjne

Przy tworzeniu wszelkiego rodzaju systemów teleinformatycznych należy pamiętać o najważniejszej rzeczy – społecznej akceptacji. System zbyt mocno ingerujący w kwestie prywatności odbiorców na pewno nie spotka się z taką aprobatą.

Niektórzy odbiorcy energii wyrażają swój niepokój związany z przetwarzaniem i przechowywaniem danych osobowych przez przedsiębiorstwa energetyczne oraz obawiają się ich ujawnienia. Zauważono, że wielu ludzi nie ufa przedsiębiorstwom energetycznym. Klienci walczą z energetyką o zachowanie ich prywatności, a sami nierzadko udostępniają dużo większą ilość prywatnych informacji. Przykładowo operatorzy telefonii komórkowej mają większą ilość danych i bardziej wrażliwe dane. Podobnie operatorzy portali społecznościowych oraz poczty internetowej. W tych przedsiębiorstwach wiedza o danym kliencie jest dużo większa niż w przedsiębiorstwie energetycznym. Tam klienci nie protestują, że jakiś podmiot przetwarza dane dużo bardziej wrażliwe niż dane pomiarowe. Co więcej – wielu ludzi umieszcza bardzo wiele osobistych informacji w takich portalach i nie przeszkadza im, że dane takie są dostępne dla innych użytkowników tych portali.

Odpowiednie przetwarzanie danych pomiarowych umożliwia ich wykorzystanie do świadczenia nowych usług. Jeżeli jednak ludzie negatywnie postrzegają przedsiębiorstwa energetyczne może to być okazja dla pojawienia się nowych graczy, np. portali społecznościowych współpracujących z przedsiębiorstwami energetycznymi. Te przedsiębiorstwa mogłyby wystąpić o zgodę na przetwarzanie takich danych, którą to zgodę klient automatycznie podpisałby bez czytania całej umowy, tak jak podpisuje wiele podobnych zgód na przetwarzanie takich danych.

Podsumowanie

Zagwarantowana prawem ochrona danych osobowych jest dobrym rozwiązaniem, jednak cyberprzestrzeń przekracza granice administracyjne państw, wraz z którymi kończy się obszar obowiązywania regulacji prawnych. Granice takie również określają obszar, w którym przestrzeganie prawa lokalnego może być egzekwowane. Pokazują jednak, że nawet najlepiej skonstruowane prawo ma zastosowanie tylko dla administracyjnie wydzielonego obszaru kraju. Konieczne staje się zatem rozwiązanie na szczeblu globalnym dla fenomenu o zasięgu globalnym – Internetu. Wydaje się bowiem, że w starciu z globalnymi gigantami internetowymi człowiek jako jednostka nie ma możliwości wyegzekwowania swoich praw. Oczywiście było kilka takich procesów, w których pojedyncze osoby uzyskały korzystny dla siebie wyrok, ale wydaje się, że zapewnienie ochrony danych osobowych (lub prywatności) nie powinno wiązać się z koniecznością prowadzenia procesu sądowego na międzynarodowych szczeblach z wielkimi przedsiębiorstwami internetowymi.

LITERATURA

[1] Cellary W.: Ile kosztuje darmowość? Wyborcza.biz 2013, http://wyborcza.biz/biznes/1,100897,14853669,Ile_kosztuje_darmowosc_.html#TRrelSST

[2] Wiewiórowski W.: Zagrożenia związane z gromadzeniem danych osobowych w inteligentnych urządzeniach pomiarowych i powiązanych z nimi bazach danych. XII edycja seminarium „Uwarunkowania wdrażania smart meteringu. Problemy prawne, technologiczne, społeczne", Warszawa 2012

[3] The Smart Grid and Privacy, Electronic Privacy Information Center 2014

[4] Czym są dane osobowe, jak interpretować art. 6 ust. 3 ustawy o ochronie danych osobowych?, http://www.giodo.gov.pl/319/id_art/973, 2009-09-17 10:16:14

SAMOLOT SZPIEGOWSKI PRZYCZYNĄ PRZERW W RUCHU LOTNICZYM USA

Pewnego dnia tuż po godzinie 15:00 czasu pacyfik (Pacific time) wystąpił problem z komputerem systemu automatyzacji lotnictwa (ERAM) w Los Angeles. Poinformowano, że automatyczne kontrolery ruchu są czasowo niezdolne do śledzenia samolotów w całej południowej Kalifornii, części Nevady, Arizony i Utah. Zakłócenie spowodowało odwołanie 50 lotów przylatujących i odlatujących z lotniska w Los Angeles oraz opóźnienie 455 lotów w całym kraju. Po szczegółowych badaniach stwierdzono, że przyczyną awarii był lot samolotu szpiegowskiego, który spowodował przeciążenie systemu komputerowego ERAM. Federalna Administracja Lotnictwa (FAA) analizuje zdarzenie, aby rozwiązać wszelkie problemy, które przyczyniły się do wypadku i zapobiec jego powtórzeniu się.

(*wb-706*) *IEEE Spectrum 2014 May*