

Uważajmy na niejawne e-profilowanie

28.01.16

Internet jest ogromnym źródłem wiedzy dla policji, służb specjalnych, operatorów telefonii komórkowej, naukowców i urzędników skarbowych. Wszystkie te instytucje są w stanie określić nasze typowe zachowania, nawet w przyszłości - twierdzi prof. Jerzy Stefanowski z Politechniki Poznańskiej. W zamian za świadczenie usług, tracimy prywatność - dodaje.



Prof. Jerzy Stefanowicz podaje przykład oferty zakładu ubezpieczeń, który w zamian za tańszą polisę daje specjalne urządzenie do samochodu, które śledzi naszą jazdę. To jest odpowiednik profilowania w internecie. Bierze się od nas w ten sposób dane jako o kierowcy. Intencja jest prawdopodobnie taka, że chodzi o przygotowanie wyspecjalizowanej oferty i wysondowanie, czy jesteśmy ryzykowanym kierowcą. Ale większość osób jest nieświadoma, że w

ten sposób powstają dane o bardzo szczegółowych fragmentach życia kierowcy. Kolejny przykład : mierniki energii elektrycznej. Dzięki nim uzyskuje się wiele osobistych danych. Tym bardziej - w internecie większość ruchów jest kompletnie nieświadoma. Obserwując ruch na stronach danego użytkownika mamy informację kim jest, co pozwoli zbudować profil jego działalności - wyjaśnia prof. Stefanowicz. Przeciętny użytkownik internetu nie sprawdza możliwości swojej przeglądarki. Jakie są metody obrony przed nieświadomym profilowaniem? Według profesora należy starać się dowiedzieć więcej o niebezpieczeństwach, czyścić historię przeglądarek, zwłaszcza z ciasteczek itd.

Prawne gwarancje

W pierwszej połowie tego roku wejdzie w życie unijne rozporządzenie dotyczące ochrony danych osobowych w internecie, które eksperci nazywają rewolucyjnym. Dlaczego?

- Przełom będzie polegał na tym, że w momencie projektowania systemu czy jednego aktu prawnego, trzeba będzie ocenić jaki wpływ będzie on miał na prywatność. Choćby domyślne ustawienia w internecie - wyjaśniała dr **Edyta Bielak-Jomaa**, Generalny Inspektor Ochrony Danych Osobowych. - Rozporządzenie wprowadzi zakaz profilowania automatycznego oraz zgodę obywatela na przetwarzanie jego danych. Kary, jakie rozporządzenie przewiduje dają

regulatorowi uprawnienia do nałożenia nawet do miliona euro za niewłaściwe przetwarzanie danych osobowych - dodała GODO.

Rozporządzenie unijne dotyczyć ma również wielkich zbiorów danych elektronicznych (Big Data). W rozporządzeniu unijnym znajdują się wyjątki od generalnych zasad ochrony np. dla służb specjalnych czy danych kościelnych. Taka konstrukcja wynika z tego, że rozporządzenie nałoży się na przepisy dyrektyw - policyjnej i sądowej, z których wynikać muszą pewne wyłączenia.

Zbiory danych w sektorze publicznym

- Nie wolno nam pozyskiwać więcej danych niż to określa ustawa o statystyce publicznej - zapewniała Agnieszka Komar-Morawska z Głównego Urzędu Statystycznego. - Zbierać dane o obywatelach można tylko w celach statystycznych, w sposób proporcjonalny przy wskazaniu wszystkich źródeł i w określonych zakresie - dodała. Tajemnica statystyczna jest tak samo silna jak tajemnica spowiedzi - podkreśliła Komar-Morawska. Dodała, że jest potrzeba stworzenia nowych przepisów prawnych, które zalegalizują korzystanie ze zbiorów elektronicznych podmiotów niepublicznych. Będzie to wyrównanie szans między sferą publiczną a prywatną.

Policja profiluje człowieka

Jak zaznaczył **dr Arwid Mednis** zbieranie danych także przez policję bardzo się zmieniło w ostatnich latach. Niegdyś policjant zbierał dane na ulicy, teraz oficer operacyjny siedzi przy komputerze i analizuje informacje w internecie. Jak daleko sięgają analizy policji przedstawił Andrzej Naperty z KG Policji.

- Organy ścigania chcą przetwarzać jak najwięcej danych, ale jest granica prawna i musimy przestrzegać Konstytucji RP. Zawsze musimy iść na kompromis, między innymi z rzecznikiem praw obywatelskich i generalnym inspektorem ochrony danych osobowych, którzy nas hamują - przyznał Naperty.

Andrzej Naperty nawiązał do nowej ustawy o Policji. Stwierdził, że musi być równowaga między ochroną prywatności a ochroną bezpieczeństwa państwa. - Dla nas Big Data, to jest wyciąganie danych, a następnie wniosków. A efektem tych prac jest profil. Profil sytuacyjny, profil człowieka, profil zachowań. Te profile są stosowane także przez inne instytucje, ale my nie możemy się tłumaczyć, że co nie jest zabronione jest dozwolone. Musimy ściśle przestrzegać reguł prawa - zaznaczył Naperty. - Śledzimy informacje na Twitterze i Facebooku, np. o nielegalnych zgromadzeniach, gdy kibice zbierają się na rozróby na podstawie profili.

Policja przetwarza dane ze źródeł uznawanych do tej pory za mało istotne. Na przykład burmistrz Nowego Jorku **Michael Bloomberg** analizuje ruch miejski pod kątem efektywnego zarządzania; remontów, sytuacji awaryjnych, wypadków.

Obchody Dnia Ochrony Danych

O tym jak zapewnić ochronę danych osobowych i prywatności w świecie Big Data, a także jakie zagrożenia i korzyści się z nim wiążą, debatowali w czwartek 28 stycznia br. uczestnicy konferencji naukowej organizowanej z okazji polskich obchodów X Europejskiego

Dnia Ochrony Danych Osobowych. Jej tematem było także unijne rozporządzenie dotyczące ochrony danych osobowych oraz wpływ zawartych w nim regulacji na możliwe zastosowania Big Data.

Konferencja odbyła się na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego. Patronem medialnym było m.in. [Wydawnictwo Wolters Kluwer](#).

[Katarzyna Żaczkiewicz-Zborska](#) 28.01.16