

Dlaczego ważni prezesi rezygnują

W codziennym życiu ilość danych, jakie generujemy na własny temat, jest dzisiaj wielokrotnie większa, niż to było jeszcze kilka lat temu. To sprawia, że **nieporównywalnie wzrasta głębokość ingerencji w naszą prywatność** – ostrzegali uczestnicy debaty DGP

Czym jest big data?

Edyta Bielak-Jomaa

Przed wszystkim to olbrzymie zbiory danych, ale jednocześnie algorytmy, przy wykorzystaniu których są one przetwarzane. Pod tym pojęciem kryją się także procesy profilowania, mówiące wiele o osobach – ich zachowaniach, przyzwyczajeniach czy podejmowanych decyzjach życiowych – co bez wątpienia oznacza olbrzymie zagrożenie dla prywatności, a z czego nie wszyscy wciąż zdają sobie sprawę. Dlatego tak istotne jest, żebyśmy już dzisiaj zaczęli rozmawiać o związanych z tym problemach, i dlatego właśnie zagadnieniom big data poświęcona jest jedna z konferencji organizowanych z okazji obchodów X Dnia Ochrony Danych Osobowych.

Arwid Mednis

Podstawową różnicą między zwykłymi zbiorami danych osobowych a big data jest chyba to, że te ostatnie nie dają się już przetwarzać tradycyjnymi metodami. Według zwolenników big data jest to zupełnie nowe podejście do metodologii badawczej. Do tej pory naukowiec stawiał sobie jakąś tezę, losował próbę i badania na tej próbie ekstrapolował na jakąś całość. Przy big data mamy do czynienia ze zmianą paradygmatu naukowego: dane za pomocą przetwarzających je algorytmów mają nam same coś podpowiadać.

Dobrym przykładem pokazującym, czym jest big data, był projekt Google Flu Trends. Na podstawie zapytań wpisywanych do wyszukiwarki Google określał, w jakich regionach geograficznych możemy mieć za chwilę do czynienia z ogniskami zapalnymi grypy.

Inny przykład świetnie obrazujący, czym jest big data, to badanie rynku motoryzacyjnego w USA, które pokazało, że najmniej wypadkowe są samochody w kolorze pomarańczowym. Oczywiście każdy od razu zastanawia się, dlaczego tak jest, ale oredowinicy big data mówią: nie róbrny tego. Dane same podpowiedzą nam, jakie są zależności pomiędzy różnymi czynnikami.

Paweł Litwiński

Z definiowaniem big data jest pewien problem: na pierwszy rzut oka nie mamy do czynienia z niczym nowym – są to po prostu informacje, także dane osobowe, które są przedmiotem przetwarzania. Ale co moim zdaniem różni big data od innych technologii przetwarzania danych? Tym elementem odróżniającym są dwa czynniki: ilość oraz możliwości. Ilość, ponieważ big data zakłada pracę na wielkich ilościach danych. W codziennym życiu ilość danych, jakie generujemy na własny temat, jest dzi-

siaj wielokrotnie większa niż to było jeszcze kilka lat temu: korzystamy z telefonu komórkowego, więc operator sieci wie, gdzie jestem, jakie strony internetowe odwiedzam, do kogo wysyłam wiadomości SMS, z kim rozmawiam itd. Możliwości natomiast wynikają ze wzrostu potencjału obliczeniowego i analitycznego komputerów.

Mogłoby się więc z pozoru wydawać, że nadal mamy do czynienia z tymi samymi informacjami, tyle, że w większej ilości. W istocie, ten wzrost ilości informacji sprawia, że nieporównywalnie wzrasta głębokość ingerencji w naszą prywatność, do jakiej może dochodzić przy wykorzystaniu tych danych.

Edyta Bielak-Jomaa

Ważna jest chyba również i nowa jakość danych i, co jeszcze ważniejsze, łatwość ich pozyskiwania. W pewnych sytuacjach generują się one same – w sposób automatyczny. Co więcej, z jednych informacji zmieniają się w inne. To pozwala na przewidywanie pewnych zdarzeń.

Andrzej Lewiński

Ja posługuję się definicją prof. Roba Kitchina z Maynooth University w Irlandii. Wskazuje on na kilka elementów. Przed wszystkim to olbrzymia ilość informacji – dla większości abstrakcyjną co do wielkości,



DR EDYTA BIELAK-JOMAA
generalny inspektor ochrony danych osobowych

liczoną w tera- i petabajtach. Kolejne elementy to wysoka dynamika, duża różnorodność, wielka szczegółowość tych danych. Dla przykładu – już teraz systemy mogą śledzić i analizować naszą reakcję emocjonalną na coś, na co patrzymy.

Nie można też zapomnieć, że w znacznej części big data to statystyka. To ona daje podstawy do wyciągania wniosków, które nie zawsze są zgodne z prawdą.

Wojciech Dziomdziora

Warto jednak zdawać sobie sprawę, że w Polsce narzędzia związane z wielkimi zbiorami danych są wykorzystywane w bardzo niewielkim stopniu. Badania pani Aleksandry Woźniak pokazały, że polskie firmy przede wszystkim opierają się na posiadanych przez sie-

bie zbiorach danych, nie sięgają do zewnętrznych źródeł. Na drugim miejscu są zachowania użytkowników na stronach internetowych firm, a dopiero na kolejnych są dane mogące wiązać z naruszeniem prywatności, np. z aplikacji mobilnych. Oczywiście w Polsce też będzie się to zmieniać, ale trzeba pamiętać, w jakim miejscu dzisiaj jesteśmy.

Nie ma jednak potrzeby odrębnej regulacji dla wielkich zbiorów danych. Tak naprawdę nie ma nawet potrzeby definiowania big data, a już na pewno nie w ustawach. Regulowane powinny być jedynie pewne aspekty związane z danymi, takie jak ich zbieranie czy profilowanie. Mamy już zresztą na stole nowe rozporządzenie unijne, które tych kwestii dotyczy.

Edyta Bielak-Jomaa

Nawet jeśli dzisiaj polscy przedsiębiorcy rzadziej niż ich zachodni konkurenci korzystają z rozwiązań big data, to bez wątpienia niebawem zaczną je stosować. Dlatego już teraz, analizując to zjawisko, warto dyskutować i starać się określić co wolno, a czego nie.

Jakie zagrożenia wiążą się z big data?

Arwid Mednis

Big data może przekreślać autonomię woli jednostki. Już dzisiaj w niektórych sklepach internetowych na podstawie danych o dotychczasowych klientach podejmuje się decyzje w stosunku do nowego klienta. Typowy przykład to podpowiedzi, jakie pojawiają się po dokonaniu zakupów. Na podstawie danych o innych kupujących sklep sugeruje mi, co jeszcze może mnie zainteresować.

Oczywiście tu jeszcze autonomia woli jednostki nie jest naruszona, bo wciąż to ja decyduję, co chcę kupić. Zdarzają się już jednak przypadki podnoszenia ceny na podstawie analizy zachowań podobnych osób. Klient, który odpowiada typowi X zapłaci mniej, a klient, który odpowiada typowi Y, zapłaci więcej. Tu już mamy do czynienia z naruszeniem autonomii woli, przy czym niekoniecznie musi to się wiązać z profilowaniem danej osoby, a może wynikać z analiz historycznych dotyczących innych.

Kolejny problem wiąże się z anonimizacją. Dane osobowe to dane, które mogą skojarzyć z konkretnym człowiekiem. Tymczasem dane zanonimizowane z jednego źródła w połączeniu z danymi zanonimizowanymi z innych źródeł mogą wskazywać konkretną osobę. Pamiętajmy, że identyfikacja nie polega na ustaleniu imienia, nazwiska i adresu, tylko na możliwości wskazania konkretnej osoby.

Paweł Litwiński

Istotna jest świadomość decyzji podejmowanej przez konsumenta – zgoda wtedy ma jakąkolwiek wartość, jeżeli została udzielona w sposób świadomy. Co jednak jeśli zgoda ta jest gdzieś zaszyta w regulaminie czy pod linkiem, który się użytkownikowi nie wyświetla? Albo jeśli użytkownik jest zmuszany do wyrażenia zgody na



ANDRZEJ LEWIŃSKI
z-ca generalnego inspektora ochrony danych osobowych

gromadzenie o nim danych, bo jeśli tego nie zrobi, to zyszczy nie będzie mógł skorzystać z danej usługi? Dlatego zgoda powinna być też wyrażana w sposób całkowicie dobrowolny i nie może być do rozumiana. Oczywiście prócz tych wymagań formalnych zgoda powinna być zyszczy nie zrozumiała dla tego, kto ma jej udzielić – bo co z tego, że konsument będzie mógł przeczytać kilka linijek całkowicie niezrozumiałego dla niego prawniczego żargonu?

Kolejne zagrożenie związane z big data to problem skali ingerencji w prywatność przy użyciu tej technologii. Inaczej trzeba oceniać prostą sytuację w rodzaju podpowiedzi, gdzie konsument znajdzie podobny towar w supermarkecie, a inaczej korzystanie z technologii, która na podstawie analizy aktywności w sieci stworzy mój profil i korzystając z niego proponuje mi filmy, które zdaniem dostawcy usług mnie zadowolą.

Andrzej Lewiński

O tym, jak głęboką ingerencję w naszą prywatność może stanowić big data, świadczą powszechnie już stosowane w USA praktyki. Jeżeli firma ubezpieczeniowa ma prawo sprawdzić wystawiane recepty czy historię choroby, to jest to niewątpliwie ingerencja zbyt daleko idąca. To jest przed nami. Wielkie korporacje ze Stanów Zjednoczonych też przecież u nas działają i chcą to robić na tych zasadach, co u siebie. Musimy się z tym liczyć chociażby w związku z negocjowanym porozumieniem

TTIP. Przy dzisiejszym poziomie codziennej inwigilacji niegdysiejsze działania Stasi są po prostu śmieszne.

Arwid Mednis

Chronione są nie tylko dane osobowe, ale również dane objęte tajemnicami sektorowymi, choćby tajemnicą telekomunikacyjną, ubezpieczeniową czy bankową. Przepisy nie mówią o tym, że tajemnicami objęte są wyłącznie dane umożliwiające identyfikację. Pojawia się więc pytanie, czy operator telekomunikacyjny może – w formie nawet w pełni zanonimizowanej – sprzedać takie dane? Hiszpańska Telefónica, która jako pierwsza zaczęła „monetyzować” dane, wyodrębniła w tym celu osobną jednostkę organizacyjną, niewykluczone że właśnie po to, by nie narazić się na zarzuty ujawniania tajemnicy telekomunikacyjnej.

Wojciech Dziomdziora

Co ciekawe, te same dane są w często posiadaniu operatora telekomunikacyjnego, który rzeczywiście niewiele z nimi może zrobić, jak i jednocześnie dostawcy oprogramowania, które użytkownik zainstaltował w telefonie. Ten dostawca już nie podlega takim ograniczeniom. To pokazuje, jak duża może być nierówność wobec prawa, także polskiego.

Nie chciałbym też, by anonimizacja była traktowana jako swego rodzaju fetysz. Wykorzystywanie danych dla tworzenia usług jest przecież korzystne dla tych konsumentów. Oczywiście oceniać prostą sytuację w rodzaju podpowiedzi, gdzie konsument znajdzie podobny towar w supermarkecie, a inaczej korzystanie z technologii, która na podstawie analizy aktywności w sieci stworzy mój profil i korzystając z niego proponuje mi filmy, które zdaniem dostawcy usług mnie zadowolą.

Edyta Bielak-Jomaa

Do tego, co już zostało powiedziane, dodałabym prawo do informacji na temat tego, kto i ile o nas wie albo chce wiedzieć. Bez tego bowiem nasze prawa podstawowe, do których należy m.in. prawo do prywatności i prawo do ochrony danych osobowych, pozostaną iluzoryczne. Co z tego, że teoretycznie mamy prawo domagać się wglądu do naszych danych czy ich modyfikacji, jeśli nie będziemy wiedzieć, że dane te w ogóle zostały zgromadzone. Od postępu technologicznego nie ma odwrotu i chyba na-

wet nie o to chodzi, by próbować go powstrzymać. Kluczowa jednak jest świadomość m.in. tego, że urzędnicy mogą nas szpiegować. To istotne, zwłaszcza w kontekście decyzji, czy się na to godzimy. Powinniśmy mieć też wiedzę, w jaki sposób możemy zablokować zbieranie dotyczących nas danych i śledzenie naszej aktywności.

Wojciech Dziomdziora

Nie można też wreszcie zapominać o bezpieczeństwie danych, bezpieczeństwie systemów informatycznych, infrastruktury krytycznej. Truizmem będzie stwierdzenie, że jako kraj jesteśmy kompletnie nieprzygotowani na cyberataki. Na razie wiemy, że minister cyfryzacji Anna Streżyńska traktuje to jako jeden ze swych priorytetów, ale będzie to wymagać wielkiego zaangażowania i olbrzymich nakładów, zarówno ze strony państwa, jak i przedsiębiorców.

Edyta Bielak-Jomaa

Z tym zagadnieniem wiążą się nie tylko zabezpieczenia techniczne, choć one oczywiście są istotne. Równie ważna jest jednak świadomość istniejących zagrożeń. Jednak zawsze słabszym ogniwem jest człowiek.

Czy powinniśmy bać się profilowania?

Paweł Litwiński

Dowiedziałem się niedawno, że dostępna jest już komercyjnie technologia badania stanu psychofizycznego użytkownika komputera na podstawie wy-



WOJCIECH DZIOMDZIORA
wiceprezes Polskiej Izby Informatyki i Telekomunikacji, radca prawny, counsel w Kancelarii Domański, Zakrzewski, Palinka

konywanych przez niego ruchów myszy. To w zasadzie klasyczny przykład zbierania danych przy okazji innych zachowań (tutaj: przy okazji korzystania ze stron internetowych), na potrzeby tworzenia big data. Od tego już w zasadzie tylko krok, by na stronach internetowych służących do zakupu ubezpieczeń oceniać mój stan zdrowia także na podstawie tego, w jaki sposób korzystam z myszki komputerowej, i od tego uzależniać cenę oferty.

To tylko przykład, ale pokazujący, że profilowanie jest czymś nieuchronnym, czymś związanym immanentnie z rozwojem techniki. I patrząc z tej perspektywy, profilowania jako konkretnych czynności w mojej ocenie nie da się zakazać: prawo nie wygra wyścigu z rozwojem techniki, prawo ze swej istoty zawsze będzie

X Dzień Ochrony Danych Osobowych

Tematowi big data będzie poświęcona odbywająca się dzisiaj na Wydziale Prawa i Administracji Uniwersyte- tu Warszawskiego konferencja zorganizowana w ramach X edycji Dnia Ochrony Danych Osobowych. Jej uczestnicy będą dyskutować o ramach prawnych przetwarzania wielkich zbiorów danych w sektorze publicznym i prywatnym, a także o nowym rozporządzeniu unijnym i jego wpływie na możliwość wykorzystania big data. Konferencja odbywa się w Collegium Iuridicum II przy ul. Lipowej 4 w Warszawie. Dziennik Gazeta Prawna sprawuje patronat prasowy nad obchodami Dnia Ochrony Danych Osobowych.

ze smartfonów

o krok w tyle. Jedynym skutecznym rozwiązaniem jest więc ocena z punktu widzenia skutku, jaki profilowanie wywołuje u osób będących jego obiektami i próba ograniczania lub nawet zakazywania korzystania z technik profilowania dla osiągnięcia niektórych celów. Tym sposobem regulacji posługuje się nowe unijne rozporządzenie w sprawie ochrony danych osobowych.

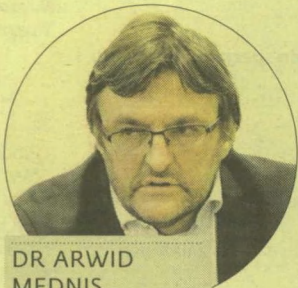
Edyta Bielak-Jomaa

Mam podobne zdanie na ten temat. Profilowani jesteście i będziemy, ale liczy się skutek i to, czy wkracza on w sferę prywatności, godności czy innych praw podstawowych człowieka. A niestety jest tak, że wkracza, bo traktowani jesteście niejednokrotnie jak potencjalni przestępcy, chociażby przez systemy używane przez służby.

Arwid Mednis

Rzeczywiście można oceniać profilowanie od strony skutków. Jeżeli przedsiębiorca oferuje mi niższą cenę, bo mieszczę się w profilu, to będzie to profilowanie. Tu jednak pojawia się problem predykcji. System na podstawie zachowań iluś osób traktuje kolejną tak

samo. Czy jednak ma rację? Niekoniecznie. I tu powracamy do zagadnienia autonomii woli, która niestety przestaje się liczyć. Już teraz niektóre polskie banki weryfikują i oceniają wiarygodność kredytową m.in. na podstawie specyficznych zakupów dokonywanych



DR ARWID MEDNIS

radca prawny, partner w Kancelarii Wierzbowski Eversheds, pracownik Wydziału Prawa i Administracji Uniwersytetu Warszawskiego

kartą. Jeśli np. ktoś kupuje alkohol w niedzielę rano, to dostanie gorszą cenę.

Edyta Bielak-Jomaa

Ktoregoś dnia może się okazać, że ktoś wpadnie na pomysł, by na tej podstawie kierować do

klubu anonimowych alkoholiczków. Dzisiaj może się to jeszcze wydawać nierealne, ale warto wiedzieć, że systemy big data stwarzają również takie możliwości.

Wojciech Dziomdziora

Nie zapominajmy jednak, że w interesie i samego banku, i jego pozostałych klientów jest jak najlepsza weryfikacja zdolności kredytowej. W interesie użytkowników dróg jest to, by policja skontrolowała trzeźwość kierowcy, dysponując danymi sugerującymi, że może prowadzić po spożyciu alkoholu. Oczywiście kierowanie na przymusowe leczenie będzie już niedopuszczalnym wkroczeniem w prywatność. Wszystko zależy od tego, gdzie wyznaczymy granice.

Arwid Mednis

Co ciekawe, zarówno w obecnej dyrektywie, jak i w projektowanym rozporządzeniu unijnym istnieje zakaz podejmowania automatycznych decyzji w stosunku do jednostki. Początkowo obawiano się, że bezduszna maszyna może się mylić, dzisiaj to wprost już wiążę się właśnie z profilowaniem. W idealnej sytuacji wspomniana

ny wcześniej kredytobiorca powinien więc zażądać od banku informacji, czym się kierowano wydając decyzję.

Andrzej Lewiński

Uważam, że prawo musi postawić tamę inwigilacji na tak masową skalę. Prowadzi ona bowiem nie tylko do zagrożeń związanych z tym, że przedsiębiorcy będą w coraz większym stopniu wykorzystywać gromadzone dane na niekorzyść konsumentów, ale także stwarza realne niebezpieczeństwa wynikające z działalności cyberprzestępców. Jak możemy godzić się na zbieranie o nas tak gigantycznych ilości informacji, mając jednocześnie świadomość, że nasze systemy teleinformatyczne nie są zabezpieczone przed atakami hakerów?

Wojciech Dziomdziora

Przy całej świadomości tych zagrożeń nie można jednak przekreślać ogromu korzyści, jakie wiążą się z big data. To nie tylko wielka szansa dla naszych przedsiębiorców, którzy będą mogli dzięki nim oferować nowe, doskonalsze usługi. To możliwość zwiększenia naszego bezpieczeństwa, możliwość

lepszego zarządzania miastami, oszczędzania energii czy zmniejszenia zanieczyszczania



DR PAWEŁ LITWIŃSKI

adwokat, ekspert Instytutu Allerhanda


środowiska. Wykorzystywanie danych wrażliwych może być przełomem w obszarze ochrony zdrowia, bo to nie tylko profilaktyka i lepsze leczenie pacjentów, ale też cała sfera badań medycznych opartych na wielkich zbiorach danych. Tych procesów nie zatrzymamy, a jeśli będziemy nadmiernie kierować się zagrożeniami, to może okazać się, że zostaniemy w tyle.

Edyta Bielak-Jomaa

Korzyści są niezaprzeczalne. Myślę jednak, że moment, kie-

dy dopiero wkraczamy w świat big data, jest właściwy, by rozmawiać z regulatorami, przedsiębiorcami, organizacjami pozarządowymi i ustawodawcą, jak osiągnąć te wszystkie korzyści przy zapewnieniu ochrony godności, prywatności i wolności człowieka. Jak chronić te wartości w bardziej innowacyjny i skuteczny sposób. Na pewno jednym z ważniejszych zadań, jakie stoją przed nami, jest też zwiększanie świadomości społecznej.

Arwid Mednis

To rzeczywiście chyba najważniejsze, by ludzie mieli świadomość, z czym wiążą się ich zachowania w internecie czy używanie przez nich różnych urządzeń. Co ciekawe, w tej chwili obserwuję chyba największy wzrost tej świadomości wśród kadry kierowniczej firm telekomunikacyjnych. Zauważyłem, że niektórzy z menedżerów zrezygnowali ze smartfonów na rzecz tych starych, małych telefonów, które pozwalają jedynie na dzwonienie i wysyłanie SMS-ów. 

Debatę przygotował

Sławomir Wikariak

Rewolucja BIG Data: Na co pozwala analiza danych **GazetaPrawna.pl**