

Z cyklu GIODO radzi...



GIODO

28 stycznia **DNIEM OCHRONY DANYCH OSOBOWYCH**

ustanowionym przez Komitet Rady Ministrów Rady Europy.

W tym roku będziemy obchodzić go po raz jedynasty. Zachęcamy Państwa do zapoznania się z treścią artykułu Kamila Nadolskiego pt. "Cyfrowa żyła złota "- Sprzedaż danych z portali społecznościowych.

Pamiętajmy, że Nasze Dane to Nasza Własność!

W załączeniu artykuł.

Globalny rynek handlu danymi osobowymi jest wyceniany na 156 mld dolarów rocznie i jego wartość ciągle rośnie. Dla brokerów danych jesteśmy jedynie produktem, który należy opakować i sprzedać.

KAMIL NADOLSKI

CYFROWA ŻYŁA ŻŁOTA

NA początku stycznia 2014 r. Mike Seay, mieszkaniec Lindenhurst w stanie Illinois, jak każdego ranka odebrał ze skrzynki korespondencji. Wśród sterty listów, ulotek i ogłoszeń reklamowych jedna koperta zwróciła jego szczególną uwagę. Przesyłka nadana przez sklep OfficeMax na naklejce adresowej miała niepokojącą adnotację: „Mike Seay, córka zginęła w wypadku samochodowym”. Koperta rzeczywiście trafiła we właściwe ręce, jako że ledwie rok wcześniej 17-letnia córka Seaya zginęła w wypadku razem ze swoim chłopakiem. Tylko skąd, do licha, wiedział o tym sklep, w którym mężczyzna od czasu do czasu kupował ryzę papieru do drukarki? Kiedy zadzwonił ze skargą, menedżer nie uwierzył i odesłał go z kwitkiem. Dopiero kiedy historię Seaya nagłośnił reporter stacji telewizyjnej NBC, firma OfficeMax przyznała, że błąd „był efektem wykorzystania listy adresowej dostarczonej przez stronę trzecią”. W końcu do mężczyzny zadzwonił z przeprosinami jeden z dyrektorów, ale mimo nalegań odmówił podania nazwy firmy rzekomo odpowiedzialnej za cały incydent. Nie powiedział też, czy posiada ona podobne informacje na temat innych potencjalnych klientów.

Przypadek Seaya to zaledwie wierzchołek góry lodowej procedury, który kwitnie od lat. Firmy handlujące danymi osobowymi, tzw. brokerzy danych, przejmują informacje pochodzące od naszych dostawców usług internetowych, wystawców kart kredytowych, operatorów telefonii komórkowej, banków, agencji kredytowych, aptek, serwisów samochodowych i sklepów spożywczych, by sprzedać je później z zyskiem. Choć z etycznego punktu widzenia taka działalność budzi wątpliwości, zasadniczo jest legalna i praktykowana na całym świecie.

DOBRE, BO DARMOWE

Niestety w większości przypadków to, co firmy wiedzą na nasz temat, jest „zasługą” nas samych. Każdego dnia zostawiamy po sobie dziesiątki cyberśladów, które brokerzy konsekwentnie gromadzą i sprzedają

za grube miliardy dolarów. Śledzenie użytkownika w sieci jest dzisiaj banalnie proste, gdyż każde urządzenie elektroniczne pozostawia własne „odciski palców”, dzięki którym każdego da się podglądać i skatalogować. Niepowtarzalne identyfikatory, tj. adres IP sieci komputerowej, za której pośrednictwem łączymy się z internetem, adres MAC karty sieciowej oraz numer IMEI lub IMSI telefonu komórkowego, umożliwiają firmom internetowym dokładne określenie, jakie urządzenia i jacy użytkownicy korzystają z ich usług.

Informacje o naszych preferencjach, mniej lub bardziej świadomie, również dostarczamy firmom sami. Zakładamy darmowe konta w serwisach społecznościowych, nie czytamy regulaminów i bezrefleksyjnie akceptujemy pliki cookies, pozwalając na śledzenie naszych ruchów. Tego typu dane są kojarzone i sprzedawane jak największej liczbie podmiotów za jak najwyższą cenę. Aplikacje w stylu Pokemon Go to najlepszy przykład na to, jak wymusić na użytkownikach permanentną możliwość geolokalizacji. Problem polega na tym, że ktoś te informacje zbiera i może je zinterpretować bez naszej wiedzy w sposób dla nas szkodliwy.

Wyobraźmy sobie, że nasz telefon komórkowy przez sześć dni w tygodniu leży na stoliku nocnym w tym samym domu, choć telefonu naszego współmałżonka. Na tej podstawie można wyciągnąć wnioski, że właściciele tych dwóch telefonów mieszkają razem, a nawet śpią w tym samym łóżku. A jeśli nasz telefon będzie leżał jeden dzień w tygodniu obok telefonu innej kobiety czy mężczyzny? Jakże wnioski mogą wyciągnąć ludzie, którzy mają dostęp do tego typu danych?

Niewiele osób się zastanawia, dlaczego takie serwisy jak Google, Facebook, Twitter, YouTube czy LinkedIn są darmowe. Większość pewnie odpowie, że chodzi o reklamy. Owszem, ale zyski serwisów z reklam to tylko część ich przychodów. Prawdziwą żyłą złota jesteśmy my sami, a właściwie dane, które generujemy o sobie. Niedawno wybuchł skandal związany z rosyjską aplikacją Prisma, zmieniającą zdjęcia w piękne obrazy. Sukces został przycięty przez „aferę”, jaka się rozpetala, gdy ktoś zapoznał się z dokładnej z polityką prywatności jej producenta. Z regulaminu jasno wynika, że Prisma Labs przejmuje od nas prawa

Ważną za korzy-
stanie z darmo-
wych aplikacji
i serwisów spo-
łecznościowych
są nasze dane.
Większość z nas
kupczy nimi bez
głębszej refleksji,
na co mogą się
kamuflować.

- 2 do przerobionych zdjęć. Co więcej, może je później wykorzystać w dowolny sposób, a użytkownik będzie dostawał co najwyżej maile z informacjami o wprowadzanych zmianach. Szkół! Tylko dla laików. Nie jest żadną tajemnicą, że podobne zasady już dawno wprowadziła większość „darmowych” serwisów.

Korzystając z LinkedIn, dajemy właścicielowi aplikacji nieodwołalny i dożywny dostęp do wszystkich informacji, które umieszczamy na stronie. Firma może je legalnie sprzedać, komu i w jakiej postaci zechce. Instagram, trzy miesiące po przejęciu przez Facebooka, ogłosił, że będzie sprzedawał nazwiska, zdjęcia i wizerunki swoich użytkowników firmom reklamowym. Posiłkując się zaktualizowanym regulaminem, serwis przyznał sobie prawo do 16 mld zdjęć zamieszczanych na swoich serwerach. W praktyce oznacza to, że każde zdjęcie opublikowane na Instagramie należy do firmy, która może je sprzedać. Nasza twarz może więc zdobić jakiś billboard, a my nie dość, że nie będziemy mieli o tym pojęcia, to w dodatku nie dostaniemy za to ani złotówki. Cieszymy się, że dzięki usłudze Google Docs możemy za darmo korzystać z arkuszy Worda i Excela?

skorzystania przez firmę z tego prawa użytkownik zgadza się oddać swoją nieśmiertelną duszę wraz z wszelkimi przynależnymi jej uprawnieniami w ciągu pięciu dni roboczych od daty otrzymania piśmennego zawiadomienia”. Na „oddanie duszy” zgodziło się 7,5 tys. osób.

CYFROWA PUSZKA PANDORY

Choć powyższy przykład można traktować w kategoriach żartu, problem wcale nie jest śmieszny. Kiedy w 2004 r. uruchomiono stronę internetową PatientsLikeMe, tysiące osób cierpiących na parkinsona, stwardnienie rozsiane, martwicze zapalenie powięzi, ostrą białaczkę limfoblastyczną, cukrzycę typu 1, HIV, stwardnienie zanikowe boczne i wiele innych poważnych chorób w końcu znalazły miejsce, gdzie mogły podzielić się swoją historią i nawiązać kontakt z ludźmi zmagającymi się z podobnymi problemami zdrowotnymi. W ciągu kilku lat strona przekształciła się w globalną społeczność ponad 200 tys. osób cierpiących na 1500 rzadkich chorób. Chorzy za pośrednictwem forum drobniaczko opisywali swoje objawy, wyniki

Kiedy wyszło na jaw, że właściciele aplikacji Priima, zmieniającej zdjęcia w piękne obrazy, roszczą sobie do nich prawa, wybuchł skandal. Problem polega na tym, że od lat robią to samo niemal wszystkie serwisy z Instagramem na czele.



A kto wczytał się w regulamin i wie, że Google ma prawa do wszystkich materiałów, które za ich pośrednictwem wytworzymy? Teoretycznie więc, gdyby J.K. Rowling napisała „Harry’ego Pottera” w Google Docs, a nie w edytorze Microsoft Word, udzieliłaby firmie Google ważnej na całym świecie licencji na wykorzystanie jej dorobku, w tym na dowolne wykorzystanie wizerunków postaci. Tym sposobem autorka odstąpiłaby Google cykl powieści warty 15 mld funtów. Sprawdza się stare porzekadło, że nie ma w życiu nic za darmo.

Aby pokazać, jak kuriozalne warunki można umieścić w umowie dotyczącej polityki prywatności, brytyjska firma Gamestation przeprowadziła eksperyment mający odowodnić, że prawie nikt nie czyta regulaminów. W warunkach udostępniania usług znalazł się ustęp: „Składając zamówienie za pośrednictwem strony internetowej Gamestation, użytkownik udziela firmie niezbędnej prawa do zażądania teraz lub w przyszłości jego nieśmiertelnej duszy. W przypadku

badan oraz wymieniali wszystkie zażywane przez siebie leki, które im przepisano. W 2010 r. pracownicy firmy BuzzMetrics skopowali zawartość wszystkich forów i przenieśli je na własny serwer. Szybko okazało się, że spółka należy do firmy Nielsen, giganta z branży reklamowej, który pozyskane informacje sprzedał koncernom farmaceutycznym. Oczywiście wybuchł skandal, choć proceder nie był nielegalny. Z powodu kontrowersji założyciele portalu postanowili jednak przypomnieć, że każdy użytkownik serwisu, klikając w okienko sugerujące zapoznanie się z regulaminem, automatycznie zgadza się na przekazywanie danych o sobie, co administratorzy PatientsLikeMe skrzętnie wykorzystywali. Serwis bowiem regularnie odsprzedał wrażliwe dane firmom z branży medycznej, które zajmują się produkcją leków, urządzeń medycznych, usługami i ubezpieczeniami.

– Każda sieć społecznościowa to nowe rejestry publiczne. Wszystko, czym się dzielimy z ludźmi

w internecie, świadomie lub nie, może być skopio-
wane, posortowane i zmagazynowane przez nowo
powstałe globalne mołochy, zajmujące się eksplora-
cją danych, a następnie sprzedane agencjom re-
klamowym, rządowi państwa i niezależnym brokerom
danych, mającym nieposkromiony apetyt na najbar-
dziej intymne szczegóły z naszego życia – ostrzega
Marc Goodman, ekspert ONZ i Międzynarodowego
Związku Telekomunikacyjnego (ITU) w dziedzinie
globalnego cyberbezpieczeństwa.

Axiom, Epsilon, Datalogix, RapLeaf, Reed Elsevier,
BlueKai, Spoko i Flurry to nazwy firm, które większość
osób niewiele mówi, ale wszystkie tworzą branżę in-
wigilacji elektronicznej, wycenianą na 156 mld dolarów
rocznie. Tylko Axiom Corporation z Little Rock posiada
ponad 23 tys. serwerów gromadzących i analizujących
evidencje danych (każdą aktywność w internecie, która
składa się na nasz profil osobowy – każdy lajk, komen-
taryz, tweet itp.), których liczba przekracza 50 mln rocznie.
Pod koniec 2013 r. Scott Howe, dyrektor generalny
firmy, przyznał dumnie, że Axiom ma profile 700 mln
konsumentów z całego świata! Każdy z nich uwzględ-
nia szereg indywidualnych cech człowieka, takich jak
rasa, płeć, numer telefonu, model samochodu, poziom
wykształcenia, liczba dzieci, powierzchnia domu, war-
tość portfela inwestycji, ostatnio nabyte przedmioty,
wiek, wzrost, poglądy polityczne, problemy zdrowotne,
zawód, a nawet lewo- lub praworęczność. Jak w prak-
tyce wygląda tak zmagazynowana wiedza, ujawniła
na przykładzie firmy Axiom Corporation Natasha
Singh, która cały proceder opisała na łamach „New York
Timesa”. Okazuje się, że Axiom przydziela każdemu
13-cyfrowy kod i – kierując się jego cechami demo-
graficznymi i stylem życia – przypisuje go do jednej z 70
kategorii osób. Przykłady? „Segment 38: Amerykanie
afrykańskiego lub latynoskiego pochodzenia, pracujący
rodzice nastoletnich dzieci należący do klasy niższej
średniej, robiący zakupy w lokalnych sklepach dyskon-
towych”. Albo inny, „Segment 48: osoby rasy kauka-
skiej, z wyższym wykształceniem, mieszkające na wsi,
ceniące życie rodzinne, zainteresowane łowiectwem,
wędkarstwem lub wycieczkami”.

Oczywiście wszystkie profile uzupełniane są do-
kładnymi danymi teleadresowymi. Bo im bardziej
szczegółowy profil, tym wyższa jego cena. Z punktu
widzenia agencji reklamowych jest to niezwykle war-
tość, bo nie od dziś wiadomo, że skuteczność reklamy
zależy od jej trafności. Pokazywanie ogłoszeń jed-
norazowych pięćdziesiąt 20-letniemu studentowi byłoby
wyrzucaniem pieniędzy w błoto, ale ta sama reklama
zaprezentowana 32-letniej ciężarnej gospodyni domo-
wej może przelozżyć się już na konkretne przychody
ze sprzedaży. Sytuacja robi się znacznie poważniejsza,
kiedy zbieranie danych na nasz temat odbywa
się z naruszeniem prawa.

EPOKA DANOINWIGILACJI

Na całym świecie mnożą się pozwawy w sprawach doty-
czących naruszenia prywatności. Są one mniej lub bar-
dziej uzasadnione, bo często nam się wydaje, że każde

wykorzystanie naszego wizerunku wymaga każdorazo-
wo naszej zgody. Zapominamy jednak, że w przypadku
serwisów społecznościowych taką zgodę już daliśmy, ak-
ceptując regulamin. Nie oznacza to, że wielkim koncer-
nem nie można niczego zarzucić. W 2012 r. prokuratorzy
generalni 38 amerykańskich stanów wytoczyli Google
proces o kradzież prywatnych danych. Koncern przy-
cisnięty do ściany przyznał, że jego samochody wyposażo-
ne w zainstalowane na dachu zaawansowane kamery
o polu widzenia 360° nie tylko robiły zdjęcia do usługi
Google Street View, ale jeżdżąc po ulicach, ściągały
dane z niezabezpieczonych sieci Wi-Fi z domów i biur:
hasła, e-maile, zdjęcia, wiadomości itd. Google tłumaczył,
że do oprogramowania wkradł się błąd, ale pod
presją prokuratorów w końcu przyznał się do kradzie-
ży. Tego typu informacje mają jeszcze większą wartość,
jeśli uświadomimy sobie, że na początku 2012 r. kon-
cern oświadczył, że łączy dane ze wszystkich swoich
70 produktów i usług w jeden profil, spośród których
wystarczy wymienić pocztę Gmail, Google Maps, Google
Calendar, Google Voice, Google Translate, Google Docs,
Google Chrome, Google Android, Google Photos (Picasa)

Regulaminowy słowotok

Fakt, że regulaminy określające politykę prywatności napisano tak,
by nikt ich nie czytał, to nie przypadek. To najczęściej długie,
pięćdziesięciostoronicowe dokumenty napisane czteropunktową czcionką
z pojedynczą interlinią i wązkiimi marginesami. Są tak zaprojektowane,
by nie dało się ich przeczytać, więc tego nie robimy. Ale możemy zapłacić
za to wysoką cenę. Z badania przeprowadzonego na Carnegie Mellon
University wynika, że przeciętny Amerykanin ma do czytania rocznie
z 1462 takimi regulaminami, a średnio mają one po 2518 słów.
Gdyby ktoś chciał przeczytać je wszystkie, musiałby poświęcić na to 76 dni,
przy czym czytałby je przez 8 godzin dziennie. Rekordowy pod tym względem
jest regulamin firmy PayPal, który liczy aż 36 275 słów. Dla porównania
„Hamlet” Szekspira składa się z 30 066.

czy Google Video (YouTube). Efekty? Zuniifikowany,
szczegółowy i bezprecedensowy obraz każdego użyt-
kownika i jego świata.

Na zarzut, że Google skanuje nasze maile, firma
odpowiedziała: „Tak jak nadawca listu do partnera
biznesowego nie może być zaskoczony, jeśli otwo-
rzy go asystent odbiorcy, tak ludzie, którzy używają
dla webowego e-maila, nie mogą być zaskoczeni, je-
śli ich komunikaty są przetwarzane przez dostawcę
usług elektronicznych odbiorcy w cyklu doręczania”.
W 2014 r. Google po analizie poczty jednego z użyt-
kowników złożył na niego donos na policję (choć na-
leży zaznaczyć, że chodziło o pedofilię).

Znacznie większy niepokój budzi handel danymi,
które zostawiamy po sobie, płacąc kartą za zakupy.
Sklepy coraz częściej wietrzą okazję i po cichu odsprze-
dają rekordy dokonywanych transakcji, bo wiedzą,
że mogą na nich zarobić często nie mniej niż na sa-
mych towarach. Warto przy tej okazji podeprzeć się

3



Cztery lata temu do amerykańskiego sądu trafił wniosek o ukaranie firmy Google, która za pomocą takich samochodów do mapowania ulic w programie Google Street View ściągała prywatne dane z niezabezpieczonych sieci Wi-Fi. Oficjalnie był to błąd w oprogramowaniu.

→ przykładem z Minneapolis, gdzie pewien ojciec dowiedział się, że jego córka jest w ciąży nie od niej samej, lecz dzięki lokalnemu sklepowi Target. Prawda wyszła na jaw, kiedy sklep zaczął wysyłać 15-latkę kupony rabatowe na asortyment ciążowy, łącznie z elementami wyprawki dla dziecka. Wściekły ojciec zrzucił menedżera, że jego córka w ciąży nie jest. Otrzymał przeprosiny, jednak podczas szczerzej rozmowy w domu usłyszał, że córka rzeczywiście spodziewa się dziecka. Tylko skąd sklep wiedział o ciąży 15-latki? Okazuje się, że na podstawie tzw. algorytmu ciąży, który analizował całą historię zakupów dokonywanych przez klientkę w świetle statystyk demograficznych kupionych od brokerów danych. Algorytm opracowano na podstawie bardzo szczegółowej analizy danych, z których wynika, że kobiety mogące być w ciąży kupują na początku drugiego trymestru więcej bezzapachowego balsamu do ciała oraz suplementów diety zawierających wapń, magnez i cynk. W sumie wskazano 25 produktów, które – wspólnie brane pod uwagę – pozwalają przypisać klientce ewentualną ciążę. Oczywiście analizować można wszystko. – Jestem przekonany, że lepiej przewidziałbym ryzyko czyjegoś zawału serca na podstawie tego, gdzie robi zakupy i gdzie jada, niż na podstawie jego genotypu

– stwierdził rozbijając Harry Greenspun, dyrektor Center for Health Solutions.

Al Gore podczas konferencji „South by Southwest”, zorganizowanej w 2013 r. w Austin, nazwał tego typu zjawiska „gospodarką prześladowania”. Inni eksperci są jeszcze bardziej dosadni i mówią o inwigilacji. Ale szefowie wielkich firm w całym procederze nie widzą niczego złego. Eric Schmidt, prezes zarządu Google, stwierdził, że jeśli robisz coś, o czym według ciebie nikt nie powinien się dowiedzieć, być może w pierwszej kolejności należałoby przestać to robić. Podobne stanowisko wyraził Mark Zuckerberg, mówiąc, że prywatność przestała być normą społeczną. Mimo deklaracji właściciel Facebooka zdaje się jednak cenić własną prywatność, bo w 2013 r. wydał 30 mln dol. na wykup czterech nieruchomości, które otaczały jego dom. Nie chciał, by ktoś mu przeszkadzał.

Frazes typu „nie mam nic do ukrycia” nie jest najlepszym punktem wyjścia do dyskusji. Nie trzeba przecież łamać prawa, by ściągnąć na siebie pewne reperkusje społeczne. Czy rzeczywiście ktoś, kto dzwoni po pomoc na infolinię dla samobójców albo przegląda w internecie porady na temat impotencji czy poszukuje adresu lokalnego oddziału Anonimowych Alkoholików, chciałby, żeby reszta świata się o tym dowiedziała? Idźmy dalej. Czy chcielibyśmy, żeby firmy ubezpieczeniowe miały wgląd w każdy nasz zakup? Jaka byłaby składka naszego ubezpieczenia zdrowotnego, jeśli ubezpieczyciel dostawałby informacje o naszych regularnych zakupach w fast foodach? A jeśli duża firma szykowałaby się do zwolnienia części pracowników, a decyzję podejmowała na podstawie algorytmów opracowanych dzięki danym kupionym od brokerów, takich jak choćby wspomniany algorytm ciąży? Oczywiście na razie to tylko rozważania, choć nigdy do końca nie wiadomo. Walmart, spółka prowadząca sieć popularnych supermarketów, już płaci firmom takim jak Castlight Healthcare za zbieranie i opracowywanie danych o stanie zdrowia swoich pracowników. Jak podkreśla jego zarząd, po to, by zachęcać zatrudnione osoby do dbania o zdrowie. Bo w ten sposób Walmart wyeliminuje zbędne koszty, zarówno te związane z leczeniem, jak i nieobecnościami w pracy.

Kamil Nadolski
dziennikarz, politolog, historyk

Artykuł pochodzi z nr 12 (grudzień 2016) gazety "Wiedza i życie" (www.wiz.pl).

Do pobrania

Załącznik	Size
1.jpgPobierz	12.13 MB
2.jpgPobierz	12.52 MB
3.jpgPobierz	5.25 MB
4.jpgPobierz	11.65 MB

25-01-2017

- [Udostępnij](#)

- [Drukuj](#)
- [PDF](#)

[Wszystkie aktualności](#)