Wojciech Rost

O ochronie danych osobowych przez portale internetowe

Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa nr 2, 75-80

2012

Wojciech ROST
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wielkopolska Wyższa Szkoła Społeczno-Ekonomiczna w Środzie Wielkopolskiej

O OCHRONIE DANYCH OSOBOWYCH PRZEZ PORTALE INTERNETOWE

Znaczenie i rola portali internetowych

Internet, począwszy od lat 90-tych ubiegłego stulecia, odgrywa stopniowo coraz większą rolę w życiu każdego Polaka. Ta „cyfrowa sieć" stanowi już nie tylko sposób kontaktu czy raczej – wymiany danych – pomiędzy ściśle określonymi użytkownikami – klientami sieci funkcjonującymi na równych prawach, co stanowiło podstawę działania protoplastów Internetu.[1] Tak jak zmieniła się struktura funkcjonowania Sieci z modelu klient – klient na dominujący obecnie model klient – serwer, tak też w niewyobrażalnym wręcz tempie rozszerzają się możliwości wykorzystania Internetu, a także funkcje, jakie spełnia. Od wprowadzenia w 1988 roku systemu internetowych pogawędek (IRC – *Internet Relay Chat*), do istotniejszych zmian z pewnością należy zaliczyć wprowadzenie tzw. „stron/portali internetowych" na początku lat 90-tych, komunikatorów internetowych od 1996 roku, systemów wymiany danych – szczególnie różnych odmian p2p (peer2peer – równy do równego; system wymiany danych typu klient – klient istniejący u protoplastów Internetu), poczty internetowej e-mail czy gier typu MMO (*Massive Multiplayer Only* – wyłącznie do masowej rozgrywki za pośrednictwem Internetu) – już w 1997 roku.

Funkcje, jakie pełni dziś Internet, powiązane są głównie, acz nie tylko, z możliwościami zastosowań różnego rodzaju stron internetowych. Pierwszą taką funkcją jest z pewnością informacyjno-publicystyczna, powiązana z istnieniem portali, a więc powiązanych ze sobą grup stron internetowych, przeważnie poszerzonych o dodatkowe funkcjonalności jak poczta, czaty, fora i inne usługi; takimi przykładowymi portalami są z pewnością Wirtualna Polska, Onet czy Interia. Chyba najbardziej znanym internetowym źródłem wiedzy jest Wikipedia – wolna (szczególnie w sensie „darmowa", udostępniona do edycji) encyklopedia, wraz z powiązanymi usługami, jak Wikicytaty, Wikisłownik, czy Wikibooks. Oprócz portali wyróżniamy także wortale – rozległe serwisy tematyczne, poświęcone określonej dziedzinie, np. technologiom – *dobreprogramy.pl*, filmom – *filmweb.pl*, etc. To nie jedyne źródła poznania informacji w Internecie, gdyż istnieją różnego rodzaju e-ziny, a więc internetowe wydania prasy. Stopniowo coraz większe znaczenie zdobywają również swoiste „dzienniki internetowe", poprzez które rozumieć należy różnego typu blogi tematyczne, np. *AntyWeb, kominek.tv*, bądź niepoświęcone konkretnej dziedzinie, będące jedynie zapisami przemyśleń ich autorów – np. na platformie należącej do Onetu *blog.pl*.

Wśród coraz szybciej rozwijających się zastosowań, aspektów Internetu, szczególne miejsce zajmuje funkcja społecznościowa, realizowana głównie poprzez portale społecznościowe jak najpopularniejszy na świecie Facebook czy rodzima Nasza-Klasa (późniejsze *NK.pl*), ale również poprzez komunikatory (coraz częściej będące swoistą częścią składową zestawu usług oferowanych przez portal, np. Facebook Chat, Gtalk/Google Hangouts). Oczywiście, choć w znacznie

[1] B. Eager, *Internet od A do Z*. Poznań 2000, s. 20-21

mniejszym stopniu, istnieje również tendencja odwrotna, jak np. w przypadku polskiego komunikatora Gadu-Gadu, który stworzył portale *mojageneracja.pl* czy *gg.pl*. Szczególnie istotną cechą tej funkcji jest fakt jej rozprzestrzeniania się w zastraszającym tempie. Coraz częściej na witrynach web figurują znaczki "Lubię to", „+1", czy wręcz możliwość zarejestrowania się do danej usługi przy użyciu danych z innego konta, istniejącego na portalu społecznościowym – przeważnie dotyczy to dwóch najpopularniejszych usługodawców w tym zakresie i oznaczone to jest „zaloguj przy użyciu konta Facebook/Google".

Funkcja społecznościowa ma na tyle istotne znaczenie, że JEDEN Z JEJ ASPEKTÓW jest wykorzystywany nawet poprzez rozwijający się wciąż e-banking (czyli usługi bankowości dostępne za pośrednictwem Internetu). Dwa z polskich, czy raczej działających w Polsce, banków aktywnie zabiegają o integrację z usługami sieciowymi, a jeden z nich ma nawet ambicję zostania „Facebookiem finansów".[2] Oprócz e-bankingu, także e-commerce zwraca uwagę na aspekt społecznościowy, umożliwiając często dostęp do produktów online poprzez zalogowanie przy wykorzystaniu konta założonego na platformie portalu społecznościowego, nie wspominając już o jego stronach reklamujących produkty na portalach społecznościowych. Szczególną formą handlu elektronicznego można nazwać różnego typu vortale „pośrednictwa pracy", jak *pracuj.pl, terazpraca.pl*, etc. Takie witryny często, oprócz „standardowych" danych użytkownika, przechowują również *curricula vitae*, które zawierają multum, często niezwykle groźnych w przypadku znalezienia się w niepowołanych rękach – co wytłumaczę w późniejszej części artykułu, danych osobowych.

Niestety, Internet w coraz większej mierze staje się komercyjny. O ile kilka lat temu było to głównie źródło wiedzy bądź kontaktu między znajomymi, o tyle obecnie na znaczeniu przybiera różnego typu rozrywka internetowa, coraz mocniej powiązana z udostępnianiem różnych danych o użytkownikach. Czy mówimy o usługach typu VOD (*Video On Demand* – „wideo na żądanie", swoisty internetowy odpowiednik dawnych „wypożyczalni kaset wideo") czy grach komputerowych, szczególnie MMO nastawionych na rozgrywkę za pośrednictwem sieci – przeważnie wiąże się to z zarejestrowaniem w serwisie oraz opłaceniem usługi za pomocą SMS-Premium, bądź przy użyciu karty kredytowej – które to dane bywają częstym celem ataków hakerów.[3]

Ostatnią funkcją Internetu, o której pragnę wspomnieć, jest *e-government,* będący w Polsce, w mojej opinii, jeszcze we wczesnej fazie rozwoju. Świetnym przykładem zastosowania e-administracji jest Estonia, w której możliwe jest wzięcie udziału drogą elektroniczną nawet w wyborach parlamentarnych. Nawet obrady Rady Ministrów mogą odbywać się za pomocą Internetu. Uważa się, że transparentność spraw publicznych, na jaką pozwala *e-government,* wpłynęła znacząco na spadek korupcji.[4] W literaturze wskazuje się jednak zagrożenia związane z taką formą administrowania, jak np. brak tajności głosowania czy możliwość manipulacji.[5]

---

[2] *http://wyborcza.biz/biznes/1,100896,11435791,100_milionow_na_nowy_mBank.html* (pobrano 29.5.2012 r.)

[3] *http://www.forbes.pl/artykuly/sekcje/wydarzenia/sony-ponownie-ofiara-hakerow,14420,1* (pobrano 11.06.2012 r.)

[4] P. Manowiecki, *W Estonii wszyscy są w Internecie*, (w:) „Gazeta Wyborcza" z 1 września 2006 r.

[5] J. Barta, R. Markiewicz, *Internet a prawo*, Universitas. Kraków 1998, s. 20

Czym są dane osobowe w Internecie i z czego wynika obowiązek ich ochrony?

Podstawowymi aktami prawnymi, które mają zapewnić bezpieczeństwo danych osobowych w Internecie są wspomniana wyżej Ustawa o ochronie danych osobowych z 1997 roku (istotnie znowelizowana w 2004 roku,[6] zwana dalej uodo), ustawa Prawo telekomunikacyjne z 2004 roku, częściowo także przepisy Ustawy o świadczeniu usług drogą elektroniczną z 2002 roku, zwanej dalej uśude. W najszerszym jednak zakresie dane osobowe chroni Kodeks Cywilny, który w artykule 23. stwierdza, że *dobra osobiste człowieka, jak w szczególności (...) nazwisko lub pseudonim, wizerunek, (...) pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach*. Artykuł 24. Kodeksu uprawnia, w przypadku naruszenia dóbr osobistych, do dochodzenia zadośćuczynienia i odszkodowania z tego tytułu.

W pewnym aspekcie, nieistotnym z punktu widzenia tego artykułu, ochrony danych osobowych dotyka także Ustawa o policji oraz Kodeksy: Karny oraz Postępowania Karnego.

Zgodnie z artykułem 6 ust. 1 ustawy o ochronie danych osobowych *za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej*. Jest to więc definicja dosyć szeroka. Z pewnością danymi osobowymi będą zatem imię i nazwisko wraz z adresem zamieszkania, określeniem wieku, ale może to również być np. adres e-mail. Są to więc podstawowe dane wymagane przez zdecydowaną większość serwisów internetowych do zarejestrowania się w nich i założenia tym samym konta, by móc korzystać z ich usług. Mimo, iż ust. 3 tego artykułu określa, że nie stanowi danych osobowych informacja, która wymagałaby nadmiernych kosztów, czasu lub działań, by na jej podstawie móc określić tożsamość osoby – zgodnie z wyrokiem Wojewódzkiego Sądu Administracyjnego w Warszawie danymi osobowymi są nawet zdjęcia z przeszłości, opatrzone przypisem z imieniem i nazwiskiem.[7]

Z punktu widzenia administratora danych osobowych (art. 7 pkt 4 uodo definiuje administratora danych jako podmiot decydujący o celach i środkach przetwarzania danych osobowych) największe znaczenie ma Rozdział 5 uodo, zatytułowany „Zabezpieczanie danych osobowych" (obejmujący artykuły 36-39a). Artykuł 36 zobowiązuje administratora danych do podjęcia wszelkich środków technicznych i administracyjnych, zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (szczególnie wrażliwe są dane dotyczące pochodzenia etnicznego, poglądów politycznych oraz inne kategorie wymienione w artykule 27 ustawy) a przede wszystkim powinien zapobiegać zapoznaniu się z nimi poprzez osoby nieupoważnione/nieuprawnione. Administrator danych powinien prowadzić również ewidencję osób upoważnionych do przetwarzania danych oraz kontrolować, komu dane są przekazywane. Z ustawy wynikają jeszcze inne obowiązki administratora danych, jak np. artykuł 26 ust. 1 pkt 4. uodo – zobowiązuje administratora do przechowywania danych pozwalających na identyfikację osób nie dłużej niż jest to niezbędne dla realizacji celu przetwarzania tych danych. Nieodpowiednie

[6] Nowelizacja nastąpiła Ustawą z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. 2004 nr 33 poz. 285), w celu dostosowania do dyrektywy 95/46/WE

[7] Wyrok NSA z 18 listopada 2009 r., I OSK 667/09, LEX nr 588798

zabezpieczenie danych osobowych sankcjonują przepisy rozdziału 8. uodo, zatytułowanego „Przepisy karne”, w odniesieniu do zabezpieczenia danych przez administratora danych są to głównie artykuły 51. określający kary za udostępnianie bądź umożliwianie dostępu do danych osobom nieupoważnionym, nawet w sposób nieumyślny oraz 52. dotyczący obowiązku zabezpieczenia danych przed zabraniem przez osobę nieupoważnioną – należy zatem wziąć pod uwagę, że nie tylko serwer powinien być zabezpieczony, ale również sama serwerownia.

W przypadku usługodawcy (określonego w art. 2 pkt 6 uśude jako podmiot, który prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy usługi drogą elektroniczną) – artykuł 6 uśude zobowiązuje usługodawcę do należytego informowania usługobiorców o szczególnych zagrożeniach związanych z korzystaniem z usługi. Istotne jest również postanowienie artykułu 8. obligujące usługodawców do określenia regulaminu świadczenia usług, który obliguje zarówno usługodawcę jak i usługobiorcę.

Zagrożenia związane z udostępnianiem danych osobowych w Internecie

Podstawowym zagrożeniem dla danych osobowych internautów są oni sami. Niestety, internauci są przeważnie osobami niecierpliwymi, które nie mają ochoty, a tym bardziej tendencji, do analizy przedstawianych im formularzy umów, które zawierają z usługodawcami. Godzą się na brzmienie regulaminów, których w rzeczywistości nie znają i w ten sposób zezwalają osobom trzecim na poznawanie ich danych osobowych, poprzez bezmyślne klikanie „Akceptuj” przy pytaniach o zezwolenie na korzystanie z określonych funkcjonalności danego konta (dotyczy to zwłaszcza gigantów: Facebook’a z jego aplikacjami dostarczanymi przez osoby trzecie oraz Google’a, który udostępnione dane wykorzystuje sam na potrzeby zleceń od reklamodawców, bądź reklamując własne usługi). Wziąwszy pod uwagę, że liczne grono osób zamiast wpisywać pełny adres w przeglądarce wpisuje jedynie interesujące ich hasło i przechodzi do interesującej ich strony z wyników wyszukiwania (przeważnie z wyszukiwarki Google) – koncern „zna nas lepiej niż własna matka” (zwłaszcza, jeśli internauta jest zalogowany na swoim koncie). Należy również pamiętać, że „to, co zostaje przesłane do Internetu – już tam zostaje”, co wynika ze struktury działania Sieci; usunięcie danych wprowadzonych w Internecie jest po prostu fizycznie niewykonalne. Dotyczy to zwłaszcza zdjęć, a niebezpieczeństwo jest tym większe, że zagrożenie może pochodzić nie tylko od nas samych, ale także naszych znajomych, którzy „tagują” (oznaczają) zdjęcia z nami. Oczywiście można wtedy, na podstawie art. 32 UODO nakazać administratorowi danych ich usunięcie, jednak ew. „szkody” mogą być już nieodwracalne.

Drugą „stronę medalu”, najgroźniejszą nawet dla świadomych użytkowników Internetu, stanowi właśnie odpowiednie zabezpieczenie danych przez osoby nimi administrujące. Oprócz wspomnianych wcześniej przepisów zobowiązujących do odpowiedniego zabezpieczania danych osobowych, art. 175 ustawy Prawo Telekomunikacyjne zobowiązuje dostawcę usług telekomunikacyjnych lub operatora sieci do zapewnienia bezpieczeństwa przekazu komunikatów w związku ze świadczonymi przez nich usługami, a także poinformowania użytkowników, zwłaszcza w przypadku szczególnego ryzyka naruszenia bezpieczeństwa świadczonych usług o tym, że stosowane środki nie gwarantują należytego

bezpieczeństwa. Niestety jednak, zdarzają się spektakularne wręcz przypadki „wycieków" danych od samych administratorów oraz nie mniej spektakularne ataki hakerskie. Wśród szczególnie dotkliwych miały miejsce m.in. wpadki polskich internetowych „pośrednictw pracy", które udostępniły zgromadzone na swoich serwerach CV,[8] żenujące pomyłki banków – np. PKO, który udostępnił dane swoich dłużników,[9] mBanku, który rozsyłał losowe przelewy wraz z danymi innych klientów,[10] czy błąd nieistniejącego już wirtualnego operatora telefonii komórkowej „GaduAir", który pozwalał na poznanie stanu konta i usług swoich „abonentów".[11]

Problem stanowi również zapewnienie ochrony danych „odpowiedniej" do zagrożeń. Szczególnie niebezpiecznym rodzajem ataku internetowego jest *phishing*, a więc wyłudzanie danych. Zdecydowanie jest też tym łatwiej wyłudzić jakieś dane osobowe, im więcej o osobie już wiemy. Z tego też względu – każdy następny atak może być coraz groźniejszy. Możliwe jest w ten sposób przejęcie internetowej kontroli nad kontem w banku, pocztą e-mail, kontem gracza czy w skrajnych przypadkach –nawet telefonem ofiary ataku [a wtedy także kontaktami i wszelkimi informacjami zapisanymi na telefonie]. Oczywiście oprócz ataków phishingu istnieją inne, znacznie bardziej wyrafinowane metody. Dlatego też odpowiednia ochrona danych osobowych, zwłaszcza w portalach internetowych, odgrywa obecnie tak ogromną rolę.

Streszczenie

Autor zajmuje się zagadnieniem ochrony danych osobowych przez portale internetowe. Obowiązek ten obciąża wszystkie podmioty administrujące danymi osobowymi, a w przypadku Internetu nabiera szczególnego znaczenia ze względu na jego ogromny rozwój i rozbudowę jego funkcji, w tym związanych z przechowywaniem i obrotem danymi osobowymi.

Punktem wyjścia jest przedstawienie w skrócie charakterystyki i rozwoju najistotniejszych funkcji i aspektów Internetu. Autor podkreśla rangę, jaką zyskuje Internet oraz ogrom możliwości, które stwarza. Następnie autor omawia podstawy prawne ochrony danych osobowych w Polsce. Są to: ustawa z 1997 roku o ochronie danych osobowych, z 2004 roku – Prawo telekomunikacyjne oraz częściowo ustawa o świadczeniu usług drogą elektroniczną z 2002 roku; najbardziej ogólną podstawą ochrony jest ustawa Kodeks Cywilny z 1964 roku.

W ostatniej części artykułu autor przedstawił analizę zagrożeń związanych z udostępnianiem danych osobowych w Internecie. Zagrożenia te można podzielić na trzy kategorie: zaniedbania użytkowników, zaniedbania administratorów danych osobowych oraz wyrafinowanie internetowych złoczyńców.

Summary

The author deals with the problem of protection of personal data by Internet portals. This duty pertains to all administrators of personal data. It is of high importance as the Internet with its functions is growing rapidly, especially functions related to collecting and saving personal data.

[8] Gigantyczny wyciek CV. GIODO zbada *terazpraca.pl; www.tvn24.pl,* (pobrano 23.05.2012 r.)
[9] Haker mimo woli, *www.tvn24.pl*, (pobrano 23.05.2012 r.)
[10] Fatalna wpadka mBanku (i Multibanku), *www.niebezpiecznik.pl*, (pobrano 16.08.2011 r.)
[11] Niebezpieczny błąd w Gadu-gadu i GaduAIR, *www.niebezpiecznik.pl*, (pobrano 17.07.2011 r.)

The author starts with a brief presentation of the characteristics and development of the most significant Internet functions and aspects. Moreover, he stresses the importance that Internet gains and the wide variety of opportunities it creates. The next part is dedicated to the legal basis for data protection in Poland. These are especially: the Law on Personal Data Protection from 1997, Telecommunications Law from 2004 and partly Law on Electronic Services from 2002; however the most general basis for the protection is the Civil Code from 1964.

In the last part the author analyzes the risks associated with sharing personal data online. These threats can be divided into three categories: negligence of users, negligence of administrators of personal data and sophistication of the Internet criminals.