Luiza Bogucka*

Bezpieczeństwo danych osobowych w świecie Facebooka

Wstęp

Bez wątpienia Facebook dokonał rewolucji w kontaktach interpersonalnych, a posiadanie profilu na tym portalu społecznościowym jest już kwestią powszechnie przyjętą w społeczeństwie. Dzięki niemu znajomi odnawiają więzi, inni utrzymują stały kontakt pomimo znacznej odległości. To właśnie Facebook zaczął powoli zastępować tradycyjne posiedzenie przy kawie koleżeńskim spotkaniem on-line. Facebook to moc możliwości dla każdego użytkownika. Mimo jego wielu zalet należy zwrócić szczególną uwagę na kwestie bezpieczeństwa danych osobowych użytkowników. Często bowiem w ferworze dobrej zabawy użytkownicy zapominają, że wszystkie treści, które udostępniają, mogą być wykorzystane przeciwko nim. Wszechobecność Facebooka w życiu każdego internauty spowodowała, że wykorzystuje się go w marketingu, polityce, do rozwoju nauki i popularyzacji czytelnictwa, stał się również doskonałym narzędziem weryfikacyjnym w procesie rekrutacji pracowników. Niemniej jednak Facebook, podobnie jak inne portale społecznościowe, nie jest wolny od zagrożeń, szczególnie tych odnoszących się do danych osobowych i wizerunku. Okazuje się, że największym zagrożeniem dla posiadaczy kont na portalach społecznościowych są oni sami. Powszechnym błędem, jaki popełniają użytkownicy, jest zasypywanie postami całego grona swoich znajomych. Wszystko po to, by pokazać swój wyidealizowany obraz, obraz człowieka sukcesu. Często udostępniane treści zawierają informacje, które oszustom mogą posłużyć do popełnienia przestępstwa. Celem artykułu jest odpowiedź na pytanie, czy przepisy dotyczące danych osobowych zapewniają odpowiednią ochronę użytkownikom i w jaki sposób przeciwdziałać zagrożeniom w sieci.

* Mgr Luiza Bogucka – Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Instytut Nauk Społecznych i Bezpieczeństwa.

Ochrona danych osobowych w świetle przepisów prawa

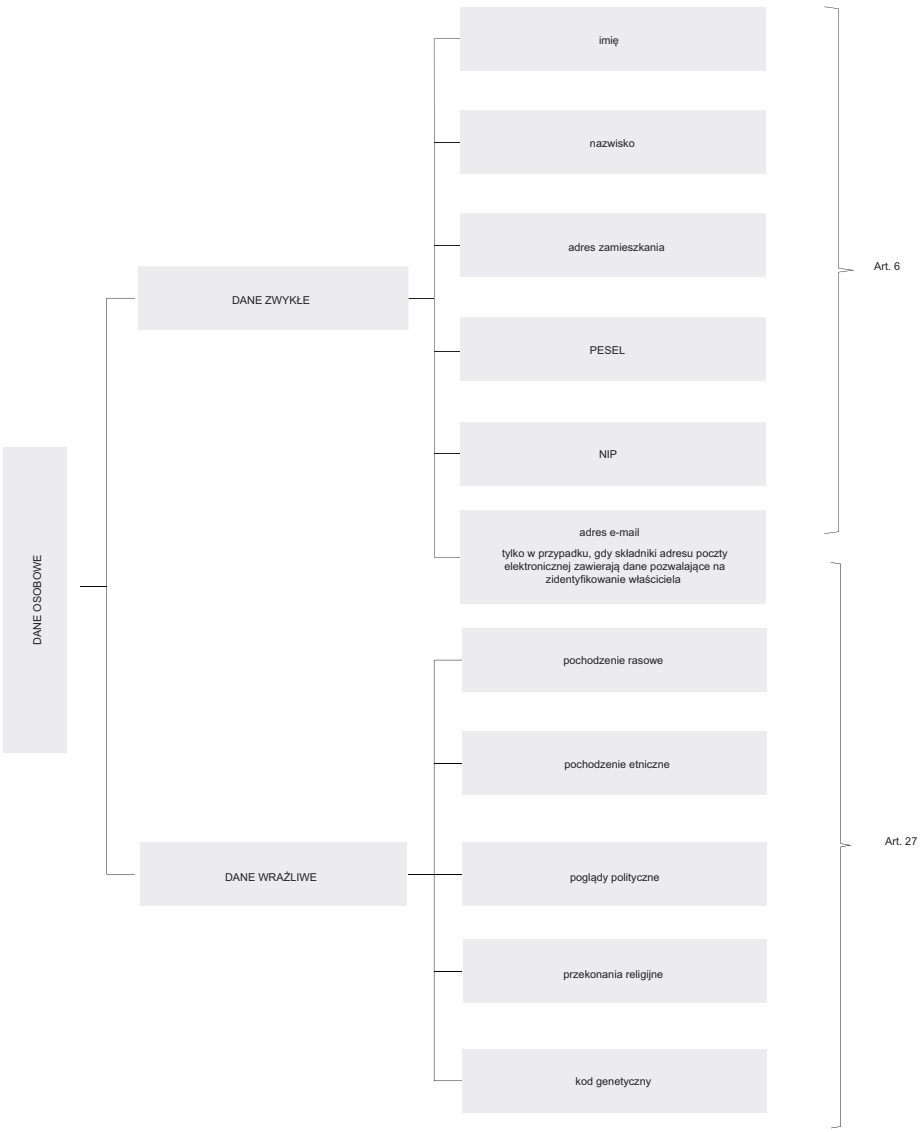
Dane osobowe (Szewc, 2007: 3–4) to termin, który na stałe wszedł do prawa polskiego za sprawą Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Zgodnie z zapisami znajdującymi się w ustawie dane osobowe to takie informacje, dzięki którym będzie można zidentyfikować osobę, tj. ustalić jej tożsamość. Osoba możliwa do zidentyfikowania to taka, 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 danej osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań (Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, art. 6.). Dane osobowe dzieli się na dane zwykłe oraz dane wrażliwe (sensytywne, szczególnie chronione). Do pierwszej grupy zaliczają się takie informacje, jak: imię, nazwisko, adres zamieszkania, PESEL, NIP oraz numer i seria dowodu osobistego. Natomiast dane wrażliwe (sensytywne, szczególnie chronione) to dane zawierające informacje o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym, skazaniach, orzeczeniach o ukaraniu mandatami, orzeczeniach wydanych przed sądem lub urzędem (Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, art. 27, ust. 1). Jest to termin potoczny, bowiem nie występuje w wyżej wymienionej ustawie.

Przetwarzanie danych podlegających szczególnej ochronie jest możliwe w przypadku, gdy obywatel, którego te dane dotyczą, wyrazi pisemną zgodę na tego typu działalność. Dopuszcza się również wyrażenie takiej zgody w wersji elektronicznej, która zawiera podpis kwalifikowany (podpis elektroniczny, który jest równoważny z podpisem własnoręcznym). Dane wrażliwe można przetwarzać m.in. w następujących przypadkach:

- działania te stanowią warunek konieczny dla ochrony żywotnych interesów;
- przepis szczególny innej ustawy zezwala na tego typu czynności;
- dane są niezbędne do dochodzenia spraw przed sądem;
- dane są wymagane do celów świadczenia usług medycznych;
- dane są niezbędne do prowadzenia badań naukowych;
- dane zostały upublicznione (podane do publicznej wiadomości) przez osobę, której dotyczą.

Zapis w Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. mówi, że „każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym", a art. 51 ustawy zasadniczej w pięciu punktach określa prawo każdego człowieka do dotyczących go danych: „1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić

i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa".



Rysunek 1. Podział danych osobowych

Źródło: opracowanie własne na podstawie Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, art. 6 i 27.

Jest to bardzo ważny zapis gwarantujący każdemu obywatelowi ochronę jego danych osobowych. Ustawa zasadnicza dała każdemu człowiekowi możliwość nieujawniania informacji dotyczących swojej osoby, zachowania prawa do prywatności.

Na straży bezpieczeństwa danych osobowych stoi Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz szereg aktów wykonawczych. Prace nad niniejszą ustawą trwały około sześciu lat i była ona pierwszym takim aktem prawnym, który w sposób kompleksowy określił zasady postępowania z danymi osobowymi (Barta, Fajgielski, Markiewicz, 2011: 98). Wraz z wejściem w życie ustawy o ochronie danych osobowych powołano Generalnego Inspektora Ochrony Danych Osobowych (GIODO), którego zadaniem jest czuwanie nad prawidłowym postępowaniem z danymi osobowymi.

Szybki rozwój portali społecznościowych, w tym niekwestionowanego lidera – Facebooka, nasuwa pytanie, czy dane osobowe użytkowników są bezpieczne. Portale społecznościowe to wirtualne miejsca, gdzie użytkownicy prześcigają się w zamieszczaniu zdjęć i zbieraniu „lajków", jest to miejsce, gdzie każdy użytkownik osiąga zamierzone cele, ma udane życie rodzinne i wspaniałą karierę, której można pozazdrościć. Każdy portal społecznościowy to miejsce, gdzie bez trudu można wykreować idealną wersję własnego „ja", wersję siebie z marzeń. Jednak w trakcie tej internetowej zabawy użytkownicy bardzo często zapominają, że Internet zachowuje wszystkie informacje w swoich zasobach. Udostępnianie informacji zawierających różnego rodzaju dane osobowe stało się poważnym problemem użytkowników. Wzmianki o życiu prywatnym zamieszczają niemal wszyscy posiadacze konta na Facebooku. Są to bardzo często dane o charakterze wrażliwym. Świat Facebooka zaczął rządzić się swoimi prawami, gdzie użytkownicy tracą zdrowy rozsądek.

Konta na portalach społecznościowych są zakładane w przeróżnych celach. Czasem serwis ten jest traktowany jako „współczesny lek na samotność", możliwość nawiązania nowych kontaktów lub utrzymania stałych relacji z innymi użytkownikami. Posiadanie konta na Facebooku wiąże się również z szybkim dostępem do wszelkich informacji. W związku ze zróżnicowaną działalnością posiadaczy facebookowych kont można podzielić na dziewięć typów:

1. Nowicjusz – świeżo upieczony użytkownik, którego można rozpoznać po jego zwiększonej aktywności.
2. Stalker – typ użytkownika, który spędza dużo czasu na portalu, obserwując innych, w tym byłych partnerów.
3. Dzielący się wszystkim – typ użytkownika, który niemal bez przerwy zamieszcza wszelkie informacje na swój temat, gdzie jest, co robi, co zamierza.
4. Wycofany – użytkownik, który zarejestrował się na portalu, często nie zamieszczając swoich prawdziwych danych lub uzupełnił profil tylko częściowo. Publikuje niewiele i dba o swoją prywatność w sieci.
5. Opiekun – udostępnia zabawne treści, przeważnie niezawierające informacji o jego życiu prywatnym; raczej skupia się na publikowaniu treści, które bawią innych.
6. Gracz skupiony przede wszystkim na dodatkowych funkcjach Facebooka – grach.

7. Baby Boomer – użytkownik, który korzysta z Facebooka sporadycznie, taktując go jedynie jako jedną z możliwości w kontaktach z dziećmi.
8. Zakochany w pracy – typ użytkownika, którego posty dotyczą sukcesów w pracy, awansów.
9. Antyużytkownik, czyli posiadacz zaniedbanego konta. Użytkownik, który ma konto, ale nie korzysta z niego, bowiem życie w sieci jest dla niego za mało atrakcyjne (*9 typów użytkowników Facebooka*, 2016).

Z analizy powyższych typów wynika, że najmniej zagrożeni są użytkownicy, którzy racjonalnie korzystają z portali społecznościowych, bądź ci, którzy korzystają z nich sporadycznie. Do tej grupy można zaliczyć typ wycofanego użytkownika oraz antyużytkownika. Te dwa przykłady charakteryzują się niewielką aktywnością, swoją działalność na portalach ograniczają do minimum, a grono ich znajomych jest poddane głębokiej selekcji. Do grona najbardziej zagrożonych użytkowników zalicza się tych najbardziej aktywnych. To oni udostępniają dużo informacji o sobie, jak również nagminnie zaznaczają miejsca, w których aktualnie przebywają. Przykładem osoby, która publikuje zbyt wiele, jest typ użytkownika dzielącego się wszystkim.

Bezpieczeństwo danych osobowych na Facebooku

W wirtualnym świecie Facebooka można znaleźć niemal wszystko. Od ogólnych informacji, po te najbardziej prywatne. Funkcjonowanie na portalu stało się już normą do tego stopnia, że duża część użytkowników zaczęła bagatelizować podstawowe zasady bezpieczeństwa, a Facebook stał się nieodłącznym elementem życia. Według danych z 2016 roku około 1,55 mld osób ma aktywne konto na Facebooku, co w porównaniu z ubiegłorocznymi wynikami można określić jako 13-procentowy wzrost. Już niemal 72% dorosłych użytkowników Facebooka korzysta z portalu przynajmniej raz w miesiącu (Zelezny, 2016).

Aby zaistnieć na Facebooku, należy podać swoje dane osobowe. Pierwszym punktem jest rejestracja, podczas której przyszły użytkownik jest proszony o zamieszczenie takich informacji, jak imię, nazwisko, data urodzenia, miejsce pochodzenia, miejsce zamieszkania, szkoły, do których uczęszczał, znajomość języków, praca, adres e-mail. W celu zakończenia rejestracji należy podać adres e-mail, który w pewnych przypadkach można uznać za dane osobowe. W zasadzie sam adres poczty e-mailowej bez dodatkowych informacji nie jest zaliczany do kanonu danych osobowych. Dzieje się inaczej, gdy jego elementy pozwalają na ustalenie tożsamości właściciela, np. w przypadku, gdy elementami adresu są imię i nazwisko lub imię, nazwisko i nazwa firmy.

Przykładem adresu poczty elektronicznej niezaliczającego się do danych osobowych jest: xyz@wp.pl. Przykład adresu poczty elektronicznej zaliczającego się do danych osobowych to: jankowalski.firmaxyz@wp.pl.

W pierwszym przypadku nie naniesiono żadnych danych, które mogłyby bez nadmiernego wysiłku określić właściciela tegoż adresu. Przypadek drugi pokazuje

jednak, że zamieszczenie takich elementów, jak imię, nazwisko i nazwa firmy pozwalają bezproblemowo ustalić tożsamość właściciela, co powoduje, że powyższy adres można traktować jako dane osobowe.

Warunkiem dokończenia rejestracji swojego profilu jest zapoznanie się z regulaminem i polityką prywatności. W toku przeprowadzonych badań na grupie 50 osób okazało się, że tylko jedna z nich odpowiedziała twierdząco na pytanie „Czy zapoznałeś się z polityką prywatności i regulaminem przed zarejestrowaniem się na Facebooku?". Oznacza to, że aż 98% użytkowników odruchowo zaznacza wymagane pola, by jak najszybciej zakończyć proces rejestracji. Z przeprowadzonych badań wynika również, że regulaminy zamieszczane na portalach społecznościowych są bardzo obszerne i często niezrozumiałe dla użytkowników. Na rutynowe już odznaczanie formuły „zapoznałem się z regulaminem" ma wpływ wiele czynników:

– liczba znajomych zarejestrowanych na danym portalu (zaufanie wzbudza sam fakt posiadania konta na danym portalu przez znajomych);
– obszerny regulamin i niezrozumiałe formuły;
– drobny tekst druku;
– przekonanie użytkowników, że każdy regulamin „jest o tym samym".

Fakt posiadania profilu przez znajomych na danym portalu społecznościowym nie oznacza, że jest on w pełni bezpieczny, bowiem każdy użytkownik musi dostosować ustawienia bezpieczeństwa (prywatności) do swoich indywidualnych potrzeb. Użytkownicy portali społecznościowych mają wiele zarzutów pod adresem regulaminów. Zapytani o przyczynę mechanicznego odznaczania wyżej wymienionej ikony odpowiadają, że regulaminy są zbyt obszerne i napisane specjalistycznym językiem, a ponadto są przekonani, że niemal wszystkie regulaminy są takie same. Część respondentów uznała, że skutecznie odstrasza ich drobny druk.

Obecnie portale społecznościowe cieszą się dużą popularnością i niemal każdego dnia zwiększa się liczba ich użytkowników. W wyniku przeprowadzonej ankiety okazało się, że niemal wszyscy posiadacze profili na portalach społecznościowych podają swoje prawdziwe dane osobowe. Jest jednak grupa użytkowników, która nie podaje rzeczywistych danych lub tylko w niewielkiej części (np. imię i pierwsza litera nazwiska lub odwrotnie). Powoduje to zawężenie grona znajomych, a tym samym zwiększenie swojego bezpieczeństwa. W grupie liczącej 480 osób 12 posiadało profil z niepełnymi lub nieprawdziwymi danymi, co według nich miało być dodatkową formą zabezpieczenia i ograniczeniem liczby znajomych do minimum (Reich, 2016: 13–21).

Na omawianym portalu społecznościowym zamieszczono regulamin i zasady obowiązujące na Facebooku, gdzie użytkownik ma możliwość uzyskania informacji dotyczących praw i obowiązków, a także zasad postępowania z danymi. Przy rejestracji każdy użytkownik jest zobligowany do zapoznania się z regulaminem, który zawiera informacje o prywatności, o tym, w jaki sposób wykorzystywane są jego dane. Ponadto autorzy tego regulaminu zwracają szczególną uwagę na działania użytkowników w zakresie bezpieczeństwa. Wyliczono bowiem szereg czyn-

ności określonych jako zakazane. W związku z tym na portalu społecznościowym Facebook nie może zarejestrować się osoba np. skazana za przestępstwo seksualne. Ponadto na serwisie zabrania się wysyłania szkodliwego oprogramowania czy wyłudzania danych, które są niezbędne przy logowaniu. Użytkownik zobowiązuje się przy tworzeniu profilu na Facebooku do podania swoich prawdziwych danych oraz funkcjonowania zgodnie z przyjętymi normami kulturalnego zachowania. Jednak aby zachować taki stan rzeczy, to przede wszystkim użytkownicy muszą działać zgodnie z regulaminem. Facebook zamieścił również zakładkę, w której znajdują się wytyczne co do zbieranych przez serwis informacji (czyli informacji o sieci, połączeniach i urządzeniach użytkowników oraz płatnościach. Zbierane są także informacje o działalności użytkownika podczas jego aktywności). Na stronie Facebooka opublikowano wiele wskazówek, które dodatkowo pomogą zapewnić bezpieczeństwo podczas korzystania z serwisu. Zwrócono tu szczególną uwagę na:

- kwestie ochrony hasła, by nie było ono oczywiste, zalecane jest utworzenie tzw. silnego hasła;
- dane dotyczące logowania nie powinny być udostępniane osobom trzecim;
- konieczność wylogowania się po zakończeniu działań na portalu;
- zalecenie zawierania facebookowej znajomości tylko z użytkownikami, których zna się w świecie realnym;
- możliwość skorzystania z dodatkowych zabezpieczeń, czyli alertów logowania i zaufanych kontaktów czy kontroli zabezpieczeń.

Bezpieczeństwo danych osobowych zależy przede wszystkim od użytkowników, ich działalności, odpowiedzialnego podejścia do kwestii korzystania z portalu oraz stosowania się do zapisów zamieszczonych w regulaminie. Mimo najlepszych zabezpieczeń do wszelkich portali społecznościowych należy podchodzić z pewną dozą nieufności i selekcjonować zamieszczane na nich informacje. Brak kontroli nad udostępnianymi treściami może stać się przyczyną wielu problemów oraz narazić użytkownika na niebezpieczeństwo.

Podsumowanie

Cieszące się szczególnie dużą popularnością portale społecznościowe z każdym dniem zyskują nowych zwolenników. Funkcjonowanie w sieci wiąże się z dużymi możliwościami, bowiem elastyczność portali i ich zdolność do dostosowywania się do współczesnych wymagań społeczeństwa to niekwestionowane zalety. Dziś zakładając profil na portalu społecznościowym, każdy użytkownik ma możliwość utrzymywania stałego kontaktu ze znajomymi oraz prowadzenia konwersacji z kilkoma osobami w tym samym czasie. Dodatkową korzyścią jest szybki dostęp do wszelkiego rodzaju informacji. Należy jednak pamiętać, by w kontaktach on-line zachować szczególną ostrożność, ponieważ dane osobowe użytkowników w niepowołanych rękach mogą stać się przyczyną wielu kłopotów.

Niemniej jednak portale społecznościowe są traktowane jako wyznacznik naszych czasów i jedna z podstawowych form komunikacji. Każdy portal, działając w trosce o bezpieczeństwo swoich użytkowników, wprowadza szereg zabezpieczeń i regulamin. Niestety nawet najlepsze zabezpieczenia ze strony portali społecznościowych są bezradne, gdy w grę wchodzi nieodpowiedzialna działalność użytkowników.

Bibliografia

9 typów użytkowników Facebooka (2016), Polityka.pl, http://www.polityka.pl/tygodnikpolityka/ludzieistyle/1600939,3,9-typow-uzytkownikow-facebooka.read?print=true, dostęp: 29.12.2016.

Barta J., Fajgielski P., Markiewicz R. (2011), *Ochrona danych osobowych. Komentarz*, Wydawnictwo Wolters Kluwer, Warszawa.

Reich T. (2016), *Jak dbać o wizerunek w mediach społecznościowych*, Wydawnictwo Słowa i Myśli, Lublin.

Szewc T. (2007), *Publicznoprawna ochrona informacji*, Wydawnictwo C.H. Beck, Warszawa.

Zelezny Ł. (2016), *Facebook – interesujące fakty*, https://socialmedia.pl/facebook-interesujace-fakty/, dostęp: 29.12.2016.

Akty prawne:

Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 2016, poz. 922.

Summary

Personal data security in the Facebook world

In the era of dynamic development of social networking sites such as Facebook, which have spread to almost every home and to every computer, it becomes an important issue to protect the personal data of its users. The article has two parts and explains the concept of personal data and its division into ordinary and sensitive data. The main objective is to answer the question whether the rules on personal data provide adequate protection for users and how to counter online threats.

Keywords: social networking site, personal data protection, Facebook, security, sensitive data

Słowa kluczowe: portal społecznościowy, ochrona danych osobowych, Facebook, bezpieczeństwo, dane wrażliwe