lic. Anna Zapiór
Wyższa Szkoła Zarządzania i Bankowości w Krakowie
azapior@o2.pl

PRYWATNOŚĆ, A KORPORACJE – BEZPIECZENSTWO INFORMACJI W DOBIE NOWYCH TECHNOLOGII

Wprowadzenie

W dobie nowych technologii, które stanowią już nieodłączny element codzienności wiele osób podążając z duchem czasu zmienia swoje nawyki co raz bardziej polegając na urządzeniach elektronicznych. Tradycyjna prasa zaczęła współistnieć z jej elektronicznym wydaniem, tablety często zastępują notatniki, a kawę można zamówić i zapłacić za nią przy dotykowym monitorze bez konieczności stania w kolejce do złożenia zamówienia.

Korzyści jakie za tym idą są bez wątpienia duże – ciężką książkę zastępuje czytnik, który oferuje dodatkowe funkcje, zamiast pęku kluczy w kieszeni miejsce zajmuje *badge* – plastykowy identyfikator umożliwiający odblokowanie drzwi do wejść, do których przydzielono dostęp, a by nie nosić portfela z gotówką czy kartami, czasem wystarczy mieć przy sobie smartfon, którym można zapłacić zbliżeniowo za towary i usługi. Ponadto taki telefon daje szereg innych możliwości, jak wysłanie lub odebranie poczty elektronicznej, zlecenie przelewu bankowego czy przeglądanie wspomnianej już prasy.

W ostatnich czasach zmienił się także sposób komunikacji, co jest szczególnie widoczne w przypadku młodego pokolenia. Ludzie częściej kontaktują się ze sobą za pośrednictwem różnego rodzaju komunikatorów, aniżeli bezpośrednio spotykając się. Bardzo rozwinęło się życie wirtualne, gdzie za pomocą popularnych serwisów społecznościowych użytkownicy dzielą się informacjami o nowej pracy, niedawno odbytych wakacjach czy wreszcie tymi zupełnie prywatnymi jak narodziny potomka, choroby czy śmierci bliskiej osoby.

W tym miejscu nasuwa się jednak pytanie, czy tak przetwarzane informacje są bezpieczne i czy rzeczywiście treści udostępniane przez użytkowników trafiają tylko do tych, których sami wybrali?

1. Informacja jako cenne źródło danych.

Fakt, że podawanie informacji o nas samych jest nieraz niezbędne, nie jest rzeczą niepokojącą. Wszak organizacje zaufania publicznego tj. służba zdrowia, policja, czy inne instytucje, jak banki mogą niejednokrotnie podjąć działania związane z daną osobą dopiero po zweryfikowaniu jej danych personalnych. Są to sytuacje, które bez wątpienia wymagają podania informacji o sobie. Są także takie zdarzenia, kiedy pewne dane umieszczamy dobrowolnie.

Korzystając z urządzeń elektronicznych użytkownicy niejednokrotnie sami umieszczają swoje dane na wszelkiego rodzaju stronach bankowych, w listach elektronicznych, notatkach w telefonie i podobnych. Są to informacje podawane i zapisywane celowo. Najczęściej wynika to z wygody i praktyczności zastosowania (łatwiej zrobić przelew elektroniczny aniżeli pocztowy, czy osobiście iść do placówki banku). Innym aspektem jest umieszczanie informacji na potrzeby rozrywki. Swoje dane użytkownicy często podają przy zakładaniu kont do różnego rodzaju serwisów społecznościowych i innych usług elektronicznych. Do najczęściej wymaganych należą imię, nazwisko, data urodzenia, numer telefonu, płeć, a także adres email.

Za przykład może posłużyć jeden z najbardziej popularnych serwisów społecznościowych, jakim jest Facebook, z którego by móc korzystać należy podać wszystkie wymienione powyżej informacje oprócz adresu email[1]. Nie inaczej jest z innymi serwisami lub stronami internetowymi, które udostępniają swoje treści i aplikacje dopiero po podaniu wymaganych danych (np. czasopisma).

Wymienione dotychczas przykłady dotyczą informacji, jakie użytkownik wszelkiego rodzaju urządzeń, portali czy serwisów podaje zupełnie dobrowolnie i celowo, a które zwykle dotyczą jego danych personalnych.

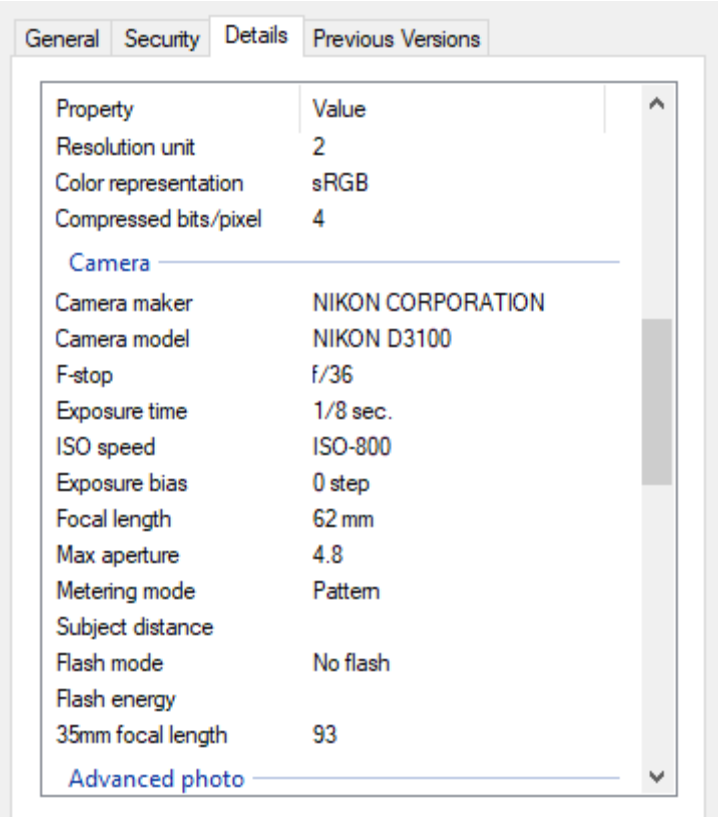
Innym rodzajem informacji są np. dane z nadajnika GPS. Najczęściej są one wykorzystywane w takich aplikacjach jak mapy na telefonie, prognoza pogody (aplikacja automatycznie wyświetla informację z pogodą dla konkretnego regionu), a nawet jako podpis lokalizacji na zdjęciu. Należy także zwrócić uwagę, iż zwykła fotografia umieszczona w Internecie także może być źródłem informacji. Można na jej podstawie ustalić nie tylko np. czas w którym została wykonana, ale także dane dotyczące sprzętu jakim ją wykonano czy nawet miejsce, jeśli aparat miał wówczas włączoną lokalizację GPS. Trzeba bowiem pamiętać, iż aparaty oprócz samej fotografii zapisują także inne dane, które znajdują się w pliku *EXIF*

[1] Facebook.com (dane wymagane na dzień 17.05.2018)

(ang. Exchangeable Image File Format – przyp. aut.) (rys. 1 i 2), w którym umieszczane są takie informacje jak:

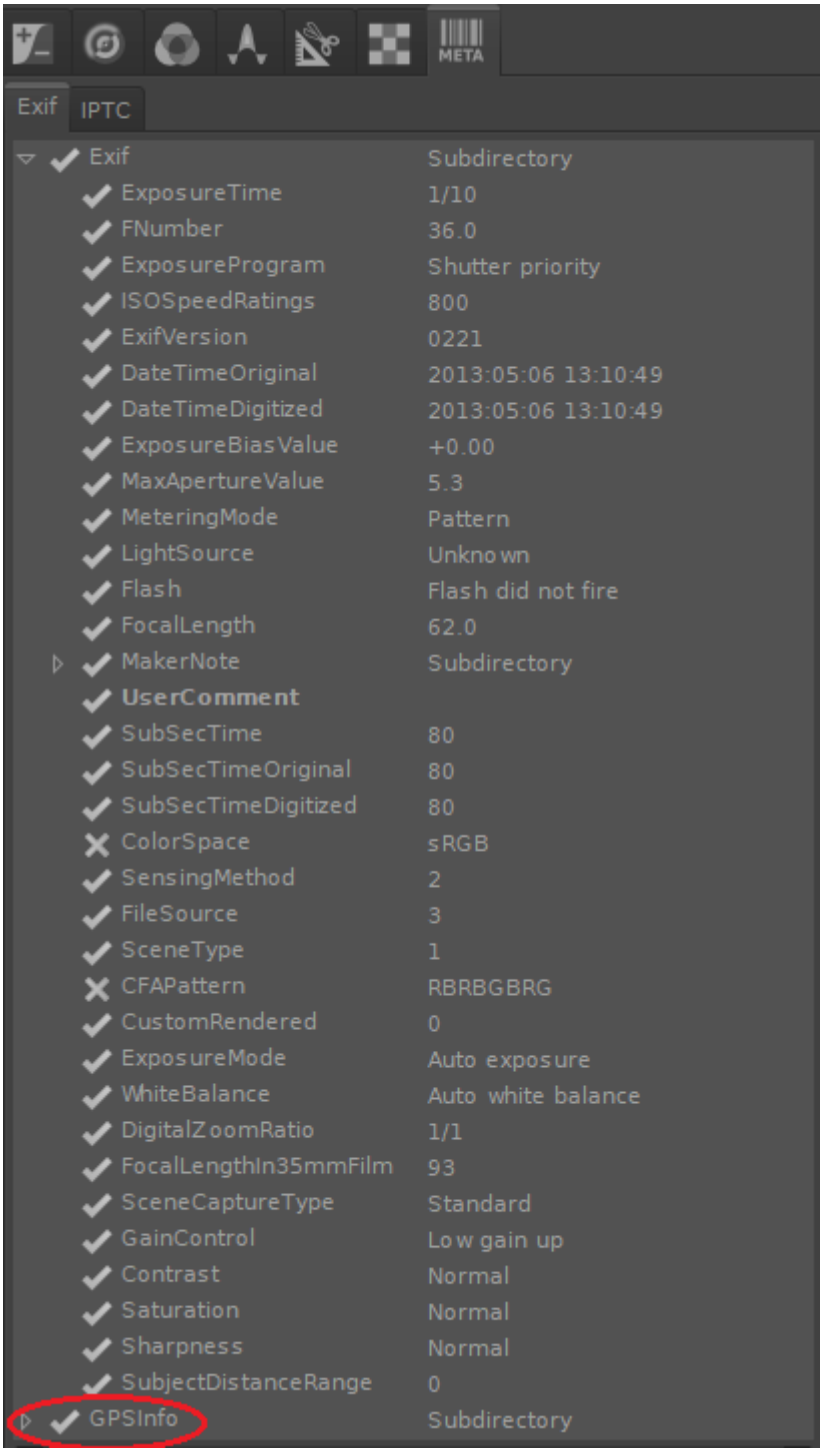
- Rodzaj urządzenia jakim wykonano zdjęcie,
- Szczegóły dotyczące zdjęcia (np. czas naświetlania, ustawienie balansu bieli, czułość ISO, wartość przysłony, ogniskową obiektywu, czas naświetlania…),
- Datę wykonania zdjęcia,
- Rozmiar zdjęcia i rozdzielczość,
- Lokalizację (jeśli włączono GPS) i inne.

Rysunek 1. Dane *EXIF* losowego zdjęcia odczytane w systemie Windows 10



Źródło: opracowanie własne

Rysunek 2. Dane pliku *EXIF* odczytane w programie RawTherapee



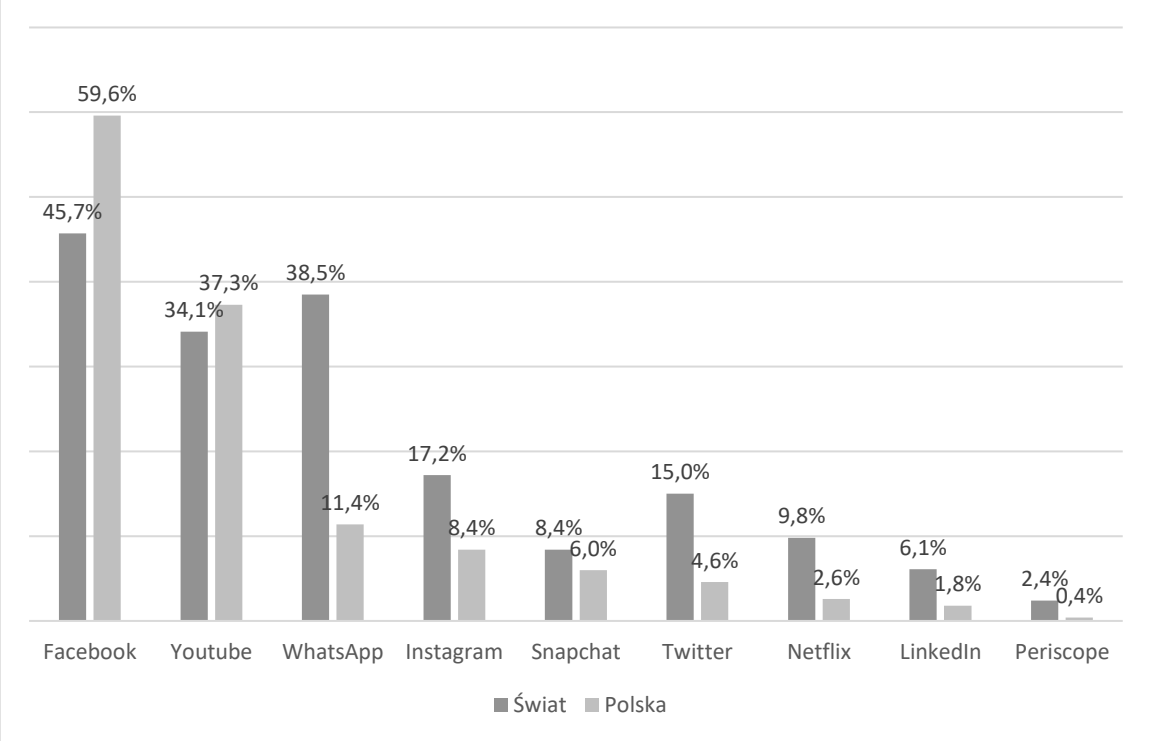
Źródło: opracowanie własne

Biorąc pod uwagę popularność niektórych serwisów i portali, niepokoi jednak ilość informacji, które użytkownicy umieszczają sami o sobie. Do Internetu trafiają takie dane jak miejsce i rodzaj wykonywanej pracy, informacje o byłych i obecnych pracodawcach, a także te dotyczące sposobu spędzania wolnego czasu, rodzaju słuchanej muzyki, czytanych książek,

zdjęcia z wizerunkiem nie tylko osób je publikujących, lecz także ich bliskich i znajomych, czy informacje dotyczące często odwiedzanych miejsc. Nie dziwi już także umieszczanie zdjęć ze szpitali, kościołów, czy cmentarzy.

Aby zrozumieć skalę i potęgę mediów społecznościowych, warto przyjrzeć się statystykom, które najlepiej obrazuje poniższy wykres.

Wykres 1. Z jakich platform i aplikacji korzystasz przynajmniej raz dziennie



Źródło: „Business Insider Polska", *Facebook nie ma sobie równych w Polsce. Tak wypadamy na tle reszty świata* (dane z 2017 r). *D*ostęp internetowy: https://businessinsider.com.pl/media/internet/najpopularniejsze-serwisy-spolecznosciowe-w-polsce-i-na-swiecie/m9gksls , data dostępu: 18.05.2018

Skala publikowanych informacji jest ogromna, niestety użytkownicy nie zawsze do końca zdają sobie sprawę z zagrożeń jakie za tym płyną. Warto jednak zwrócić uwagę na zupełnie inną rzecz dotyczącą przekazywania informacji o użytkowniku. Wiadomo już bowiem, że oprócz informacji podawanych świadomie i dobrowolnie, są także te, które są zapisywane automatycznie (jak wspomniany przykład pliku *EXIF*), a także te pozyskane w sposób

nielegalny. Poniżej przedstawiono kilka przykładów firm, których analiza daje jednoznaczne wnioski dot. bezpieczeństwa danych użytkowników, a także sposobu zbierania informacji.

2. Sposoby pozyskiwania i wykorzystywania informacji na przykładzie wybranych firm

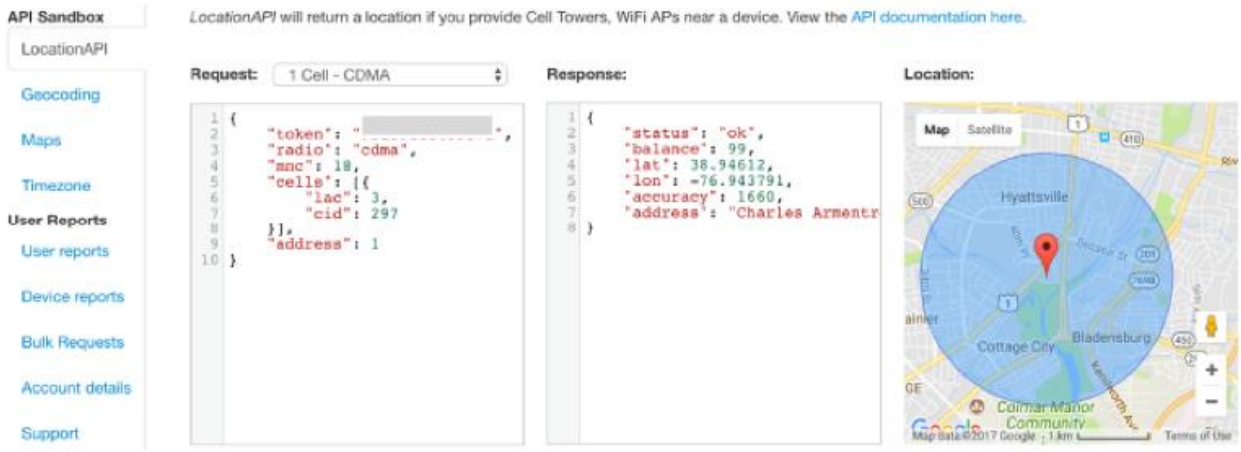
Jako pierwszy warto przytoczyć przykład firmy Google. Jak podaje magazyn Quartz[2], firma ta od początku 2017 roku za pośrednictwem smartfonów z systemem Android zbierała informacje o położeniu najbliższych wież telekomunikacyjnych, następnie przesyłano je za pośrednictwem Internetu na serwery Google (rys.3). Dane te były zbierane nawet wówczas, gdy telefon nie miał włączonej usługi lokalizacyjnej, ani włożonej karty SIM. Praktyki te potwierdził sam rzecznik firmy pisząc:

„W styczniu tego roku [2017 – przyp. aut.] zaczęliśmy za pośrednictwem kodu ID telefonów szukać dodatkowego sygnału, by poprawić wydajność i szybkość dostarczania wiadomości”[3].

W tym miejscu należy zauważyć, iż każdy telefon ma unikalny numer identyfikacyjny, który można powiązać z danymi z lokalizacji z wież. Istotne jest także, że o ile dane z jednej wieży nie dadzą zbyt dokładnej informacji o położeniu telefonu, o tyle w oparciu o dane z kilku nadajników można już z dość dużą precyzją ustalić położenie urządzenia.

Rysunek 3. Lokalizacja nadajnika telekomunikacyjnego wyssana do Google

[2] Keith Collins, Google collects Android users’ locations even when location services are disabled, 21.11.2017 dostępny w Internecie: https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/. Data dostępu: 06.05.2018
[3] Ibidem, (tłumaczenie własne).



Źródło: Quartz, https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/

Pozostając przy firmie Google warto także wspomnieć o praktykach nagrywania użytkowników za pomocą ich własnych smartfonów[4]. W tym przypadku, podobnie jak poprzednio firma posłużyła się smartfonami z systemem Android. Urządzenie reagując na losowo wypowiedziane słowo „*google*" nagrywało przypadkowe rozmowy osób znajdujących się w jego pobliżu, a tak zapisane rozmowy przechowywano jako pliki audio. Co ciekawe pliki te można było odsłuchać, a aby to zrobić wystarczyło wejść na stronę *history.google.com* w zakładkę „Voice & audio". Można było je także skasować w ustawieniach konta, a także zablokować w telefonie opcje dotyczące nagrywania, lecz i w tym przypadku firma robiła to bez wyraźnej zgody użytkowników, a w konsekwencji mało kto wiedział o takiej możliwości.

Niestety korporacja znana głównie z wyszukiwarki, nie jest jedynym przedsiębiorstwem, które korzystało z danych pozyskanych od swoich klientów bez ich wiedzy. Nie sposób pominąć w niniejszej pracy firmy Cambridge Analytica (CA), która, jak ujawniło śledztwo dziennikarskie prowadzone przez dziennikarzy „The New York Times", a także brytyjski „The Guardian" i „The Observer", łamiąc prawo weszła w posiadanie informacji o niemal 50 milionach użytkowników Facebooka.

[4] Joanna Dobosiewicz„ *Google nagrywa nasze rozmowy. Pliki można odsłuchać*, "Business Insider Polska", 14.02.2018. Dostęp internetowy: https://businessinsider.com.pl/technologie/nowe-technologie/google-przechowuje-pliki-dzwiekowe-zfragmentami-naszyc-rozmow/cen2yzy, data dostępu: 18.05.2018

Cała sprawa miała swój początek w 2014 roku, gdy, jak podaje „Business Insider”[5] jeden z pracowników CA, Aleksandr Kogan stworzył aplikację pozwalającą na przewidywanie osobowości użytkownika. Aplikacja „thisisyourdigitallife”, bo tak ją nazwano, w zależności od ilości tzw. „polubień” zostawianych w mediach społecznościowych określała preferencje konkretnej osoby. Im więcej „polubień” dana osoba zostawiała, tym trafniejszy był model jej osobowości. Początkowo aplikację udostępniono użytkownikom Facebook’a, którzy, wyrażając zgodę poddali się badaniu, a wyniki, jak wstępnie zapewniano miały posłużyć wyłącznie celom naukowo-badawczym. W ten sposób zebrano dane dotyczące ok. 270-320 tys. osób. Następnie Cambridge Analytica za pośrednictwem powiązanych ze sobą spółek podpisała umowę na przechowywanie i przetwarzanie danych użytkowników Facebooka, pobierając już nie tylko wyniki osób uczestniczących w badaniu, ale także ich znajomych i osób z nimi powiązanych. Szacuje się, że brytyjska firma weszła w ten sposób w posiadanie danych prawie 50 milionów użytkowników. Co więcej, jak wskazuje magazyn „Das Magazine”[6], model stworzony do analizowania osobowości użytkowników w sieci, prawdopodobnie nie został stworzony przez wspomnianego profesora Aleksandr’a Kogan’a, lecz skopiował on jedynie model dra Kosińskiego. Tak zebrane dane, jak podaje „Business Insider”[7] miały przyczynić się do wyjścia Wielkiej Brytanii z Unii Europejskiej, a także wygranej Donalda Trump’a w wyborach prezydenckich w 2016 roku w USA.

Ostatnim przykładem przytoczonym w niniejszej pracy, z uwagi na jej ograniczoną objętość jest Kaspersky Lab – jedna z najbardziej znanych na świecie firm produkujących oprogramowanie antywirusowe. Firmę posądza się o szpiegowanie na rzecz Rosji, a sytuacja jest o tyle kuriozalna, iż de facto to szpiedzy nakryli szpiegów. Sprawę opisały obszernie na swoich łamach „The New York Times”[8] i „The Wall Street Journal”[9], które podają, iż sprawa ta została ujawniona po tym, jak izraelskie służby przeszukując serwery Kaspersky’ego zauważyły, iż ktoś już wykorzystuje oprogramowanie tej firmy do szpiegowania komputerów

[5] Brennan Weiss, *Trump-linked firm Cambridge Analytica collected personal information from 50 million Facebook users without permission*, “Business Insider”, 18.05.2018
[6] Von Hannes Grassegger, Mikael Krogerus, *Ich habe nur gezeigt, dass es die Bombe gibt*, “Das Magazin”, 03.12.2016.
[7] Brennan Weiss, *Trump-linked firm Cambridge Analytica collected personal information from 50 million Facebook users without permission*, “Business Insider”, 18.05.2018.
[8] Nicole Perlroth, Scott Shane, *How Israel Caught Russian Hackers Scouring the World for U.S. Secrets*, "New York Times", 10.10.2017. Dostęp internetowy: https://www.nytimes.com/2017/10/10/technology/kaspersky-labisrćl-russia-hacking.html, data dostępu: 18.05.2017
[9] Shane Harris, Gordon Lubold, Paul Sonne, *How Kaspersky’s Software Fell Under Suspicion of Spying on America*, “The Wall Street Journal”, 05.01.2018. Dostęp internetowy: https://www.wsj.com/articles/howkasperskys-software-fell-under-suspicion-of-spying-on-america-1515168888, data dostępu: 18.05.2018

użytkowników popularnego antywirusa. Przeszukiwanie owych komputerów nie miało jednak na celu znalezienia złośliwego oprogramowania, lecz dokumenty. Co więcej poszukiwano takich z klauzulą „ściśle tajne". W ten sposób – jak można przeczytać w „NYT" - przeszukano komputery ok. 400 mln użytkowników. Warto zaznaczyć, iż w owym czasie z oprogramowania znanej, rosyjskiej firmy korzystały takie instytucje w USA, jak Departament Obrony, Sprawiedliwości, Departament Stanu, Departament Skarbu, Armii i Sił Powietrznych, a także Departament Energii. Powołując się na wspomniane wcześniej źródło, w ten sposób uzyskano dostęp do ściśle tajnych dokumentów przechowywanych przez jednego z pracowników NSA (Agencji Bezpieczeństwa Narodowego – przyp. aut.), który przechowywał je na swoim prywatnym komputerze. Dosyć absurdalne wydaje się być w tej sytuacji zarządzenie NSA, która zabroniła swoim pracownikom korzystać z oprogramowania Kaspersky Lab, gdyż, jak podaje „The New York Times", sami wykorzystywali je do operacji hackerskich, zatem wiedzą jakie stanowi zagrożenie dla nich jako agencji.

Na koniec warto zwrócić uwagę, iż sama firma Microsoft, po zalogowaniu do jednego konta oferuje dostęp do takich usług i produktów jak Skype, OneDrive, Xbox Live, Bing, Outlook, MSN. Na każdym z nich przechowywane są inne dane jak kontakty (Skype), dane do karty płatniczej (Xbox Live), czy prywatne wiadomości z email'i, na które wysyła się przecież także takie informacje jak wyniki badań. Jak podaje Wikipedia „w czerwcu 2012 roku z LinkedIn wyciekło 6,5 mln haseł użytkowników Linkedin"[10], który w 2016 r. został przejęty przez Microsoft. Nietrudno zatem wyobrazić sobie do jakich danych (ze wskazaniem na ich ilość, a także wartość) można uzyskać dostęp po zalogowaniu tylko do jednego konta i jakie mogłyby być konsekwencje w przypadku ich kradzieży.

Podsumowanie

Jak wskazano w punkcie pierwszym niniejszego artykułu, w sieci Internet nie trudno znaleźć dane dotyczące konkretnych osób, wykonywanego przez nich zawodu, miejsc, które ostatnio odwiedzili i znajomych z którymi się spotykają. W wyszukaniu tych informacji pomocne są takie strony, jak wspomniany już Facebook, a także LinkedIn, Instagram, czy Pinterest. Umieszczając tam zdjęcia, aktualizując profil o nowe miejsce pracy, czy relacjonując wycieczkę, użytkownicy często nie zdają sobie sprawy z faktu, iż dane te łatwo zebrać i

[10] Wikipedia.pl, dostęp internetowy: https://pl.wikipedia.org/wiki/LinkedIn. Data dostępu: 18.05.2018

stworzyć z nich profil określonej osoby. Nie wymaga to także dużego wysiłku, czy czyjejś zgody, gdyż informacje często są dostępne publicznie.

Natomiast przytoczone w punkcie drugim *case studies*, choć nieliczne, pozwalają przynajmniej w małym stopniu ocenić bezpieczeństwo informacji umieszczanych w Internecie, choć właściwiej byłoby napisać o jego braku. Przykładów tak nieetycznych zachowań firm, jak podane, można by mnożyć jeszcze długo.

Istotą sprawy nie jest jednak popadanie w skrajności, snucie teorii spiskowych, a w konsekwencji zaprzestanie korzystania z wszelkiego rodzaju urządzeń elektronicznych, lecz świadome i mądre ich używanie. Czytanie regulaminów, rozważne zamieszczanie informacji na swój temat w sieci Internet, a także informowanie o zagrożeniach bliskich, ze szczególnym uwzględnieniem najmłodszego pokolenia.

Literatura:

[1] Business Insider Polska, https://businessinsider.com.pl/media/internet/najpopularniejsze-serwisy-spolecznosciowe-w-polsce-i-na-swiecie/m9gksls.

[2] Tamże, https://businessinsider.com.pl/technologie/nowe-technologie/google-przechowuje-pliki-dzwiekowe-zfragmentami-naszyc-rozmow/cen2yzy.

[3] Cadwalladr C., Graham-Harrison E., Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, "The Guardian", 18.05.2018.

[4] Confessore N., *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, "The New York Times", 18.05.2018.

[5] Grassegger V. H., Krogerus M., Ich habe nur gezeigt, dass es die Bombe gibt, "Das Magazin", 03.12.2016.

[6] Knaus C., Just 53 Australians used Facebook app responsible for Cambridge Analytica breach, "The Guardian", 18.05.2018.

[7] „The New York Times", https://www.nytimes.com/2017/10/10/technology/kaspersky-labisrćl- russia-hacking.html.

[8] "The Wall Street Journal", https://www.wsj.com/articles/howkasperskys-software-fell-under-suspicion-of-spying-on-america-1515168888.

[9] Quartz, https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/.

[10] Weiss B., Trump-linked firm Cambridge Analytica collected personal information from 50 million Facebook users without permission, “Business Insider”, 18.05.2018.

[11] Wikipedia, https://pl.wikipedia.org/wiki/LinkedIn.

Streszczenie

Niniejszy artykuł ma na celu zwrócić uwagę na zagrożenia płynące z wykorzystywania nowych technologii, a przede wszystkim z nadmiernego umieszczania informacji na wszelkiego rodzaju serwisach społecznościowych. Wskazano w nim także sposoby zbierania i wykorzystywania informacji o użytkownikach przez firmy takie jak Kaspersky Lab, Facebook, czy Google, a także zwrócono uwagę na ich nieetyczne zachowania wobec użytkowników i klientów.