Jak wiele informacji o sobie udostępniamy w Internecie

Paulina Brzęcka 184701 Marek Borzyszkowski 184266

27 marca 2025

SPIS TREŚCI

1. WSTĘP I CEL RAPORTU

W dobie powszechnej cyfryzacji coraz więcej aspektów naszego życia przenosi się do świata wirtualnego. Codziennie korzystamy z mediów społecznościowych, wyszukiwarek internetowych, aplikacji mobilnych i wielu innych platform, nie zawsze zastanawiając się, jakie informacje o sobie udostępniamy i jakie mogą być tego konsekwencje. Dane, które pozostawiamy w sieci - świadomie lub nieświadomie - mogą obejmować zarówno podstawowe informacje, takie jak imię i nazwisko, wiek czy miejsce zamieszkania, jak i bardziej wrażliwe dane, takie jak zainteresowania, preferencje zakupowe czy historia przeglądania stron. Współczesny Internet sprawia, że budowanie profilu użytkownika na podstawie dostępnych informacji jest niezwykle łatwe, a same dane mogą być wykorzystywane na różne sposoby przez rozmaite podmioty.

Niniejszy raport ma na celu analizę skali i sposobów udostępniania danych w Internecie. W kolejnych rozdziałach omówiona zostanie budowa profilu użytkownika na podstawie podstawowych informacji, źródła pozyskiwania danych oraz sposoby ich wykorzystywania przez firmy, instytucje i inne organizacje. Szczególna uwaga zostanie poświęcona zagrożeniom wynikającym z nadmiernego udostępniania informacji, takim jak kradzież tożsamości, nieuprawnione śledzenie aktywności czy manipulacja preferencjami użytkowników. W końcowej części raportu przedstawione zostaną rekomendacje dotyczące ochrony prywatności i minimalizacji ryzyka związanego z publikowaniem danych w sieci.

1.1. Cel pracy

Celem niniejszego raportu jest zbadanie, w jakim stopniu i w jaki sposób użytkownicy Internetu udostępniają swoje dane oraz jakie niesie to za sobą konsekwencje. Szczególny nacisk zostanie położony na analizę różnych źródeł informacji, mechanizmów zbierania danych oraz podmiotów, które je przetwarzają i wykorzystują. Poprzez dokładne przeanalizowanie tego procesu możliwe będzie wskazanie zagrożeń związanych z nadmiernym udostępnianiem informacji oraz ocena, w jakim stopniu użytkownicy mają nad nim kontrolę.

Drugim, równie istotnym celem raportu, jest przedstawienie praktycznych zaleceń dotyczących ochrony prywatności w Internecie. Omówione zostaną sposoby minimalizowania ilości udostępnianych danych, techniki zabezpieczania informacji oraz narzędzia, które mogą pomóc w ochronie tożsamości cyfrowej. Ostatecznym efektem pracy będzie zwiększenie świadomości czytelników na temat zagrożeń i sposobów zabezpieczenia swoich danych w sieci, co pozwoli im podejmować bardziej świadome decyzje dotyczące własnej prywatności.

2. ŹRÓDŁA POZYSKIWANIA INFORMACJI

2.1. Identyfikacja i analiza publicznie dostępnych źródeł [1]

W dobie powszechnego dostępu do Internetu oraz ogromnej popularności mediów społecznościowych, zdobycie informacji na temat osoby prywatnej, przedsiębiorcy czy pracownika jest dziś łatwiejsze niż kiedykolwiek wcześniej. Użytkownicy często sami - świadomie lub nieświadomie - pozostawiają po sobie szereg danych, które można wykorzystać do stworzenia precyzyjnego profilu.

Według raportu „Digital 2021" (We Are Social i Hootsuite), z Internetu w Polsce korzysta 31,97 mln osób, a 25,9 mln aktywnie używa mediów społecznościowych. To oznacza, że większość społeczeństwa codziennie generuje cyfrowe ślady, które mogą być później analizowane.

2.1.1. Media społecznościowe [2]

Facebook, Instagram, X, LinkedIn czy Snapchat gromadzą dane zarówno świadomie podawane przez użytkowników (np. miejsce pracy), jak i te zbierane automatycznie - lokalizacja, adres IP, urządzenia. Dane mogą pochodzić także z aplikacji firm trzecich, programów lojalnościowych czy partnerów marketingowych.

Szczegółowe zestawienie, jakie dane są gromadzone w mediach społecznościowych zostały przedstawione w poniższej tabeli. [3]

Zakres danych / Działanie	**Facebook**	**X**	**LinkedIn**
DANE OSOBOWE			
Imię i nazwisko	+	+	+
E-mail	+	+	+
Numer telefonu	+	+	+
Data urodzenia	+	+	+
Adres zamieszkania	+	+	+
Poprzednie miejsca zamieszkania	+		
Zdjęcia profilowe	+	+	+
Rodzina i związki	+		
Wykształcenie	+		+
Języki obce	+		+
Poglądy polityczne	+		
Przekonania religijne	+		
Wydarzenia z życia	+		
DANE ZAWODOWE I LOKALIZACYJNE			
Miejsce pracy	+		+
Kwalifikacje	+		+
Wynagrodzenie			+
Płatności	+		+
Lokalizacja	+	+	+
Urządzenia	+	+	+
Adres IP	+	+	+

Kalendarz			+
ŹRÓDŁA POZYSKIWANIA INFORMACJI			
Od użytkownika	+	+	+
Od innych użytkowników	+	+	+
Od partnerów zewnętrznych	+		+
Z aplikacji zewnętrznych	+	+	
Z aktywności (kliknięcia)	+	+	
ZASTOSOWANIA I UDOSTĘPNIANIE			
Reklamy	+	+	+
Personalizacja	+	+	+
Oznaczanie na zdjęciach	+		
Meldowanie w lokalizacjach	+	+	
Sugestie kontaktów	+		+
Udostępnianie firmom	+	+	+
Cele badawcze i analityczne	+	+	+

Jesli chodzi o Facebook, to gromadzi on najszerszy zakres danych - zarówno prywatnych, jak i zawodowych, w tym dane kontaktowe, lokalizacyjne, relacyjne i behawioralne. Dane są również pozyskiwane od partnerów i aplikacji zewnętrznych. Warto zaznaczyć, że domyślne ustawienia prywatności, których większość użytkowników nigdy dokładnie nie czyta przed akceptacją, bardzo często sprzyjają upublicznieniu informacji, a około 40% użytkowników nie zmienia nigdy ustawień prywatności, co czyni ich dane łatwo dostępnymi.

W aplikacji X domyślnie wszystkie posty (tweety) są publiczne. Dodatkowo dane gromadzone również poprzez partnerów i aplikacje zewnętrzne, a polityka firmy jest dosyć liberalna i udostępnia dane badaczom.

Firma LinkedIn dodatkowo profiluje użytkowników głównie pod kątem danych zawodowych (miejsce pracy, kwalifikacje, języki), które potem są wykorzystywane komercyjnie i sprzedawane firmom rekrutacyjnym. Może być to szczególnie niebezpieczne przy atakach typu spear-phishing, gdzie precyzyjne informacje są używane do podszywania się i oszustw.

2.1.2. Fora, sekcje komentarzy, blogi

Uznawane za „anonimowe", w rzeczywistości łatwe do deanonimizacji. Powtarzające się pseudonimy, zdjęcia profilowe, adresy IP - wszystko to pozwala powiązać konto z konkretną osobą, po mniej lub bardziej wnikliwym poszukiwaniu.

2.1.3. Rejestry publiczne i portale firmowe [4]

Z racji powszechnej cyfryzacji, przed udostępnieniem niektórych danych w internecie nie można się uchronić. Szczególnie osoby prowadzące firmy lub działalności gospodarcze, a nawet osoby posiadające nieruchomości. Nie wspominając o tym, że prawie każdy dorosły człowiek w dzisiejszych czasach pracuje w jakiejś firmie, gdzie często dane kontaktowe, adresy e-mail, a czasem także numery telefonów pracowników czy właścicieli firm są udostępniane na stronie firm, bardzo często nawet bez wiedzy samych zainteresowanych.

Niektóre dane są dostępne w postaci rejestrów internetowych:

- **CEIDG** - zawiera dane o jednoosobowej działalności gospodarczej, w tym adres, który nierzadko

jest miejscem zamieszkania.

- **KRS** - dane zarządu, często z numerem PESEL, umożliwia pozyskanie numeru PESEL i daty urodzenia członków zarządu spółek.
- **CRBR** - udostępnia dane beneficjentów rzeczywistych, w tym numery PESEL udziałowców spółek.
- **Elektroniczne Księgi Wieczyste** - umożliwiają dotarcie do danych właścicieli nieruchomości.
- **Portale ogłoszeniowe, firmowe** - e-maile, telefony, nazwiska

2.1.4. Urządzenia IoT

Inteligentne urządzenia domowe (głośniki, żarówki, lodówki) zbierają dane o rutynie, lokalizacji i obecności użytkownika. Coraz więcej urządzeń domowych (np. tostery, żarówki, głośniki) jest wyposażanych w moduły internetowe. Nawet jeśli nie oferują realnych funkcji online, dane z nich są zbierane i mogą być wykorzystywane marketingowo. Koszt wdrożenia łączności IoT dla producenta jest niewielki, a dane mają wysoką wartość.

> „Kupując sprzęt domowy, możemy nieświadomie nabyć urządzenie IoT. Kluczowym zasobem są dane - które mogą zostać sprzedane lub wykorzystane przez producenta." - Mikko Hypponen

2.1.5. Czat AI jako nieświadome źródło informacji [5]

Coraz więcej osób korzysta z narzędzi opartych na sztucznej inteligencji (AI), takich jak ChatGPT czy Bing Chat, aby wspierać się w pracy zawodowej. Według badań aż 43% pracowników używa AI do realizacji swoich zadań. Choć AI oferuje wygodne i szybkie odpowiedzi, istnieją zagrożenia dotyczące prywatności i bezpieczeństwa danych, o których warto pamiętać, że:

- dane mogą być przetwarzane lub analizowane przez ludzi,
- platformy zastrzegają prawo do przechowywania zapytań,
- AI modele, takie jak ChatGPT, mogą uczyć się na podstawie zadawanych pytań. Dlatego nie powinno się wprowadzać do nich żadnych danych osobowych ani poufnych.

Co zdarza się ludziom udostępnić, a nie powinno się tego robić:

- Imię i nazwisko,
- Data urodzenia,
- Adres zamieszkania,
- Numer dowodu osobistego,
- Telefon, adres e-mail,
- Kod źródłowy lub dane z projektów w fazie rozwoju,
- Poufne informacje o produktach i usługach,
- Niezaprezentowane jeszcze pomysły lub rozwiązania,
- Numery kart kredytowych,
- Numery kont bankowych,
- Hasła i dane logowania,
- Wyniki badań,

- Diagnozy lekarskie,
- Informacje dotyczące leczenia.

Aby korzystać z AI w sposób odpowiedzialny i bezpieczny, warto stosować się do kilku prostych zasad:

- Używanie jedynie informacji ogólnodostępnych i nieidentyfikujących,
- Podawanie dane fikcyjne lub zanonimizowane, jeśli konieczne jest podanie przykładu.
- Nie publikowanie szczegółowych planów podróży lub wakacji — może to narażać na kradzież lub inne ryzyko offline.
- Założenie drugiego, anonimowego konta, które nie jest powiązane z właściwą tożsamością.
- Korzystanie z bezpiecznego połączenia internetowego — unikanie otwartych sieci Wi-Fi w kawiarniach czy hotelach.
- Nie udostępnianie haseł ani nie proszenie AI o ich generowanie na potrzeby konkretnej usługi.
- Zachowanie ostrożności przy danych zdrowotnych, finansowych i prywatnych,
- Zapoznanie się z regulaminem i polityką prywatności chatu AI,
- Sprawdzenie, jakie dane są przechowywane, jak długo i komu mogą być udostępniane,
- Zwrócenie uwagi, czy narzędzie przewiduje możliwość przeglądu zapytań przez człowieka w celach jakościowych.

2.2. W jaki sposób dane trafiają w niepowołane ręce?

Chociaż skoro myślimy, że udostepniamy bardzo mało danych, bądź wcale, istnieją aktualnie techniki, które są na tyle zaawansowane, że na podstawie jednej, bądź kilku informacji można stworzyć czyiś profil osobowy. Do jednej z nich zalicza się biały wywiad. Open Source Intelligence, cyli biały wywiad, to wyspecjalizowana technika polegająca na analizie dostępnych publicznie informacji w celu identyfikacji i gromadzenia danych o wybranej osobie.

- przeszukiwanie stron internetowych pod kątem danych kontaktowych,
- wyszukiwanie kont społecznościowych na podstawie adresu e-mail lub loginu,
- analizę zdjęć w celu rozpoznania wizerunku i odnalezienia powiązanych treści,
- korelowanie fragmentarycznych danych z różnych źródeł (np. fora, blogi, komentarze).

Aktualne narzędzie umożliwiają bardzo wnikliwą analizę, między innymi:

- automatyczne przeszukiwanie domen internetowych w celu odnalezienia adresów e-mail,
- sprawdzanie, na jakich portalach społecznościowych zarejestrowano konkretne nazwy użytkowników,
- analizę zdjęć za pomocą sztucznej inteligencji w celu identyfikacji osoby.

Chociaż prawda jest taka, że nie potrzeba żadnych profesjonalnych narzędzi, aby komuś uprzykrzyć życie. Dostęp do danych wrażliwych może mieć każda osoba prywatna, wystarczy tylko odrobina negatywnej motywacji oraz chwila czasu spędzona na poszukiwaniu i wnioskowaniu, ale o tym wiecej w nastepnych rozdziałach.

3. ZAGROŻENIA

3.1. Zagrożenia wynikające z udostępniania danych

Współczesne organizacje i użytkownicy indywidualni coraz częściej stają się ofiarami zagrożeń wynikających z niekontrolowanego udostępniania danych. Informacje osobiste mogą zostać wykorzystane zarówno przez zewnętrznych atakujących, jak i osoby z wewnątrz firmy — obecnych lub byłych pracowników, kontrahentów, a nawet przypadkowych użytkowników popełniających błędy.

3.1.1. Kradzież tożsamości

Udostępnienie danych osobowych, takich jak imię, nazwisko, PESEL, numer dowodu czy adres e-mail, może skutkować:

- podszywaniem się pod ofiarę w celu zaciągnięcia pożyczki, otwarcia konta bankowego czy przeprowadzenia transakcji,
- wykorzystaniem danych w oszustwach ubezpieczeniowych, zdrowotnych lub podatkowych,
- długoterminowymi problemami finansowymi i prawnymi ofiary.

Przykład z życia: W ataku na Marriott w 2020 r. wyciekło ponad 5 mln rekordów gości, zawierających dane kontaktowe, urodziny i numery kont lojalnościowych.

3.1.2. Naruszenie prywatności i poufności danych

Dane, które zostaną ujawnione — nawet nieświadomie — mogą naruszyć prywatność pracowników, klientów czy partnerów biznesowych. Skutki to:

- utrata kontroli nad własnymi informacjami,
- możliwość ich dalszego rozpowszechniania,
- narażenie na nieautoryzowane monitorowanie.

Przykład z życia: były pracownik Tesli w 2023 r. ujawnił dane ponad 75 000 pracowników, w tym numery SSN i informacje finansowe.

3.1.3. Cyberstalking i nękanie

Gdy dane kontaktowe lub lokalizacyjne stają się publiczne, rośnie ryzyko:

- śledzenia i nękania w sieci lub w świecie rzeczywistym,
- stosowania szantażu lub gróźb,
- prób kontaktu ze strony osób niepożądanych, np. stalkerów.

Przykład z życia: lokalizacja kobiety w Japonii po odbiciu w oku na zdjęciu.

3.1.4. Oszustwa socjotechniczne i internetowe

Ujawnione dane są wykorzystywane do:

- phishingu (fałszywe e-maile i strony),
- spear-phishingu (ukierunkowane ataki na konkretną osobę),
- vishingu (oszustwa telefoniczne),

- przekonywania ofiar do ujawnienia loginów i haseł.

Przykład: w 2020 r. grupa atakujących uzyskała dostęp do systemów Twittera, podszywając się pod pracowników i kradnąc dane do kont znanych osób.

3.1.5. Konsekwencje reputacyjne

Dla osób publicznych, pracowników wysokiego szczebla lub właścicieli firm, ujawnienie danych może prowadzić do:

- utracenia zaufania klientów i partnerów,
- negatywnego rozgłosu medialnego
- trudności w znalezieniu nowej pracy lub rozwijaniu kariery.

Przykład: wyciek danych w firmach takich jak Proofpoint, Apple czy Google nadszarpnął ich wizerunek jako liderów w dziedzinie innowacji i bezpieczeństwa.

Przykład: dane z Facebooka w 33% spraw rozwodowych.

3.1.6. Odpowiedzialność prawna

Udostępnianie danych bez zgody lub ich niewłaściwe zabezpieczenie może skutkować:

- pozwami cywilnymi ze strony poszkodowanych osób,
- karami finansowymi za naruszenie przepisów o ochronie danych (np. RODO/GDPR),
- odpowiedzialnością dyscyplinarną lub karną.

Przykład: Microsoft mógłby zostać ukarany grzywną do 20 mln euro za wyciek danych z systemów GitHub, gdyby doszło do naruszenia danych klientów z UE.

3.2. Przykłady rzeczywistych incydentów [6, 7]

- **David Quintavalle** - błędnie oskarżony na podstawie zdjęcia.
- **Angela Dunnn** - protesty po ujawnieniu adresu.
- **Guy Babcock** - fałszywe oskarżenia o przestępstwa seksualne.
- **Yue Chen** - ustalenie adresów lekarzy do planowania ataku.

4. ZALECENIA DOTYCZĄCE PRYWATNOŚCI

4.1. Jak się chronić? [8]

Nadmierne lub nieświadome udostępnianie danych może narazić nas na poważne zagrożenia, takie jak kradzież tożsamości, oszustwa czy cybernękanie.

4.1.1. Adres e-mail i numer telefonu

Zagrożenia: spam, phishing, ataki socjotechniczne, przejęcie kont.
Rekomendacja: używaj oddzielnego e-maila do rejestracji; nie udostępniaj numeru telefonu publicznie.

4.1.2. Adres domowy i lokalizacja geograficzna

Zagrożenia: ryzyko włamania, śledzenia, identyfikacji miejsca zamieszkania.
Rekomendacja: wyłącz geolokalizację w aplikacjach; unikaj publikowania informacji o podróżach czy codziennej rutynie.

4.1.3. Zdjęcia nieletnich

Zagrożenia: wykorzystanie zdjęć przez osoby nieuprawnione, ryzyko ich rozpowszechnienia bez zgody.
Rekomendacja: dokładnie przemyśl publikację zdjęć dzieci; ustaw ścisłe ograniczenia prywatności.

4.1.4. Kompromitujące zdjęcia

Zagrożenia: *sextortion* (szantaż zdjęciami), cyberprzemoc.
Rekomendacja: nigdy nie udostępniaj intymnych zdjęć, nawet zaufanym osobom — tracisz nad nimi kontrolę.

4.1.5. Dokumenty osobiste

Zagrożenia: kradzież tożsamości, oszustwa finansowe.
Rekomendacja: nie publikuj dokumentów tożsamości, umów czy informacji bankowych; jeśli musisz przechowywać je online — szyfruj dane.

4.1.6. Opinia, skargi i kontrowersyjne komentarze

Zagrożenia: naruszenie reputacji, konflikty, nękanie.
Rekomendacja: przemyśl każdą publikację; internet nie zapomina, a wypowiedzi mogą być błędnie zinterpretowane.

4.1.7. Prywatne rozmowy

Zagrożenia: ujawnienie poufnych informacji, ryzyko naruszenia prywatności innych osób.
Rekomendacja: korzystaj z szyfrowanych komunikatorów; nie przesyłaj wrażliwych danych w czatach.

4.2. Bezpieczny dostęp do internetu i mediów społecznościowych

- **Skonfiguruj ustawienia prywatności** na swoich kontach - ogranicz widoczność treści tylko do osób zaufanych.
- **Używaj silnych, unikalnych haseł** - regularnie je zmieniaj i nie używaj ich wielokrotnie.
- **Uważaj na podejrzane linki** - sprawdzaj źródło wiadomości i nie klikaj w nieznane odnośniki.
- **Korzystaj z zaufanych źródeł cyberbezpieczeństwa** - np. Incibe, OSI.

Twoje dane to Twoja odpowiedzialność.
W świecie cyfrowym prywatność nie jest dana raz na zawsze - trzeba ją stale chronić.

WYKAZ LITERATURY

[1] "Jakie ślady zostawiamy w internecie?" (Dostęp 2025-03-26). [Online]. Available: https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1019082,prywatnosc-w-internecie.html.

[2] "Twitter, snapchat, internet rzeczy. dane konsumenta na wyciągnięcie ręki," (Dostęp 2025-03-26). [Online]. Available: https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1017004,twitter-snapchat-iot-czyli-dane-konsumenta-na-wyciagniecie-reki-2000.html.

[3] Wiesław Wolny. "Bezpieczeństwo i prywatność danych w badaniach mediów społecznościowych," (Dostęp 2025-03-26). [Online]. Available: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.cejsh-06278ad0-d165-4b1c-8b2b-5817b3982416/c/07.pdf&ved=2ahUKEwjqnLHL35SMAxUwMRAIHewwFJAQFnoECBEQAQ&usg=AOvVaw3qYoSnGsBD_Z3EekwfDAoJ.

[4] "Co wie o nas internet?" (Dostęp 2025-03-26). [Online]. Available: https://www.infor.pl/prawo/prawa-konsumenta/konsument-w-sieci/5297247,Co-wie-o-nas-Internet.html.

[5] "Things you shouldn't share with chatgpt," (Dostęp 2025-03-26). [Online]. Available: https://telefonicatech.com/en/blog/things-you-shouldnt-share-with-chatgpt.

[6] "11 real-life insider threat examples," (Dostęp 2025-03-26). [Online]. Available: https://www.mimecast.com/blog/insider-threat-examples/.

[7] "10 times someone's online information made them unsafe in real life," (Dostęp 2025-03-26). [Online]. Available: https://www.linkedin.com/pulse/10-times-someones-online-information-made-them-unsafe-bridges.

[8] "Protect yourself online: Data you should never share," (Dostęp 2025-03-26). [Online]. Available: https://telefonicatech.com/en/blog/data-you-should-never-share-how-to-protect-it.