Komunikacja społeczna

Semestr Letni 2025

Prywatność współczesnej komunikacji

Boris Komarov - 268959

Spis treści

1 Wprowadzenie

W czasach, gdy komunikacja za pośrednictwem nowoczesnych technologii odgrywa ogromną rolę, a niemal każdy korzysta z jakiegoś rodzaju komunikatora, pytania o prywatność danych stają się coraz bardziej powszechne. Ludzie coraz częściej zastanawiają się, jakie uprawnienia mają poszczególne aplikacje zainstalowane na ich urządzeniach oraz w jaki sposób przechowywane są ich dane.

Ale czy naprawdę warto przejmować się prywatnością? Niektórzy twierdzą, że nie mają nic do ukrycia, podczas gdy firmy oferujące usługi zapewniają, że wszystko jest szyfrowane – lub, gdy dochodzi do ujawnienia danych na żądanie, tłumaczą to działaniem na rzecz dobra ogółu.

W tym tekscie postaram się przybliżyć temat prywatności danych oraz pomóc w znalezieniu równowagi pomiędzy ochroną prywatności a wygodą korzystania z nowoczesnych technologii.

2 Jak to działa

Cokolwiek trafia do internetu, prawdopodobnie już w nim pozostanie. Dlatego, jeśli nie planujesz dzielić się jakąś informacją, lepiej jej w ogóle nie umieszczać w sieci. Mając to na uwadze, możemy przejść do mniej oczywistych kwestii.

2.1 Poczta

Poczta elektroniczna w swoim pierwotnym założeniu nigdy nie była projektowana z myślą o bezpieczeństwie czy prywatności. Na początku służyła jedynie do prostej wymiany informacji pomiędzy pracownikami tego samego biura w zaufanym środowisku lokalnym. Nie przewidywano potrzeby uwierzytelniania nadawcy, szyfrowania wiadomości ani ochrony prywatności – wiadomości były przesyłane otwartym tekstem [7].

Sytuacja uległa zmianie, gdy e-mail zyskał dostęp do internetu i zaczął być powszechnie używany. Brak zabezpieczeń stał się poważnym problemem: każda wiadomość mogła zostać przechwycona, odczytana, a nawet sfałszowana.

2.2 Pretty Good Privacy

W odpowiedzi na te zagrożenia, amerykański programista Phil Zimmermann opracował w latach 90. algorytm PGP (Pretty Good Privacy). Był on zaniepokojony faktem, że każdy mógł czytać cudze wiadomości e-mailowe i postanowił temu przeciwdziałać. PGP wykorzystuje kryptografię asymetryczną (klucze publiczne i prywatne), dzięki czemu tylko nadawca i odbiorca mogą odszyfrować zawartość wiadomości. Było to jedno z pierwszych dostępnych publicznie narzędzi zapewniających rzeczywiste szyfrowanie end-to-end.

Rząd Stanów Zjednoczonych zareagował na rozwój PGP bardzo negatywnie. Ponieważ algorytm był zbyt silny, by dało się go łatwo złamać, uznano go za narzędzie o potencjalnym znaczeniu militarnym i objęto kontrolą eksportową, jak broń. Zimmermann został objęty śledztwem pod zarzutem naruszenia ustawy o kontroli eksportu broni (Arms Export Control Act) [12]. Aby uniemożliwić jego zakazanie, postanowił opublikować kod źródłowy PGP w formie książki — co uniemożliwiło rządowi skuteczne zablokowanie rozpowszechniania tego narzędzia.

Od tego momentu znaczenie silnego szyfrowania zaczęło rosnąć. Narzędzia takie jak PGP odegrały kluczową rolę w popularyzacji idei prywatnej komunikacji i doprowadziły do powstania bardziej bezpiecznych protokołów, takich jak HTTPS. Chociaż PGP do dziś pozostaje jednym z najbezpieczniejszych systemów szyfrowania wiadomości, jego złożoność ogranicza masowe użycie, zwłaszcza wśród nietechnicznych użytkowników.

2.3 Messengery

Wiele dzisiejszych komunikatorów, takich jak WhatsApp, Messenger czy Telegram, chwali się stosowaniem szyfrowania end-to-end (E2E). Oznacza to, że wiadomość jest szyfrowana w momencie jej wysłania i może zostać odszyfrowana wyłącznie na urządzeniu odbiorcy. W teorii nawet firma zarządzająca serwerami nie ma dostępu do treści tych wiadomości, ponieważ dane na serwerze przechowywane są w formie zaszyfrowanej.

3 Dane są szyfrowane, więc chyba w porządku?

Nie do końca. Istnieje wiele technik szyfrowania danych, jednak równocześnie rozwijane są metody ich obejścia lub złamania. Przykładem jest strategia znana jako Harvest Now, Decrypt Later (HNDL), w której nawet silnie zaszyfrowane dane są gromadzone z myślą o ich przyszłym odszyfrowaniu – na przykład przy użyciu przyszłych technologii, takich jak komputery kwantowe [14].

Warto również zauważyć, że sama obecność szyfrowania nie gwarantuje pełnej ochrony. Jednym z głównych zagrożeń są tzw. podatności końcowe (endpoint vulnerabilities) – czyli sytuacje, w których urządzenie nadawcy lub odbiorcy zostaje naruszone, co pozwala uzyskać dostęp do danych przed ich zaszyfrowaniem lub po odszyfrowaniu [2].

Dodatkowo, niektóre firmy technologiczne są poddawane naciskom ze strony rządów, aby wdrażały backdoory, czyli celowe luki w zabezpieczeniach. Tego typu rozwiązania mogą umożliwiać instytucjom państwowym dostęp do danych użytkowników bez ich wiedzy [2, 7, 9].

4 Czemu udostępniają dane?

Firmy technologiczne udostępniają zebrane dane z kilku głównych powodów – najczęściej są to względy finansowe oraz wymogi prawne.

Z punktu widzenia finansów, dane użytkowników stanowią podstawę wielu modeli biznesowych. Informacje o lokalizacji, historii przeglądania, preferencjach czy aktywności w mediach społecznościowych są wykorzystywane do tworzenia profilowanych kampanii reklamowych. Firmy zarabiają, oferując reklamodawcom precyzyjnie dobraną grupę odbiorców. Dane mogą być też przekazywane lub sprzedawane zewnętrznym podmiotom - takim jak brokerzy danych czy partnerzy afiliacyjni. Przykładowo, Facebook i Google byli oskarżani o skanowanie prywatnych wiadomości oraz analizowanie treści e-maili w celach reklamowych [4, 11].

Z kolei względy prawne obejmują zarówno lokalne przepisy, jak i międzynarodowe regulacje. Władze państwowe mogą zobowiązać firmy do udostępnienia danych użytkowników poprzez nakazy sądowe, wezwania do sądu lub inne procedury administracyjne. Agencje rządowe, takie jak FBI, DHS czy ICE w USA, regularnie uzyskują dane od firm technologicznych, m.in. w celach dochodzeniowych, wywiadowczych czy przy weryfikacji wizowej. Podobne naciski mają miejsce również w Europie – przykładem jest Wielka Brytania i jej Investigatory Powers Act 2016, który pozwala państwu wymuszać osłabienie zabezpieczeń kryptograficznych [19, 5, 7].

Jednocześnie firmy muszą przestrzegać regulacji dotyczących ochrony danych osobowych, takich jak RODO (GDPR) w Unii Europejskiej czy CCPA w Kalifornii. Choć te przepisy mają na celu zwiększenie przejrzystości i ochrony prywatności użytkowników, w praktyce oznaczają również obowiązek szczegółowego zarządzania danymi i odpowiedzi na żądania organów nadzorczych [13].

5 Nie mam czego ukrywać

Argument „nie mam nic do ukrycia" często pojawia się w dyskusjach o prywatności, jednak wiele rzeczywistych przykładów pokazuje, jak złudne może być takie podejście. Osoby, które nie miały złych intencji ani nie łamały prawa, często stają się ofiarami automatycznych systemów skanowania danych i nadinterpretacji informacji. Jak trafnie zauważył Edward Snowden: "Ultimately, arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

Jednym z bardziej znanych przypadków był ojciec, który zrobił zdjęcia intymnych części ciała swojego dziecka, by przesłać je lekarzowi. Zdjęcia zostały automatycznie przesłane do Google Photos i zaklasyfikowane przez algorytmy jako materiały nielegalne, co uruchomiło zawiadomienie służb. Mimo że po śledztwie nie stwierdzono żadnego przestępstwa, mężczyzna stracił dostęp do swojego konta Google i danych z ponad 10 lat [17].

Inne przypadki dotyczą np. oprogramowania rozpoznającego twarze, które na podstawie nieprecyzyjnych danych doprowadziło do fałszywych oskarżeń, głównie wobec czarnoskórych mężczyzn [18, 16]. Firmy takie jak Amazon i Tesla również zostały przyłapane na tym, że ich pracownicy mieli dostęp do prywatnych nagrań – czasami zawierających intymne sceny – pochodzących z kamer instalowanych w domach lub samochodach [15, 6].

Warto również zauważyć, że dane raz zgromadzone mogą zostać wykorzystane w kontekstach, które dziś wydają się nieistotne, ale w przyszłości mogą prowadzić do realnych konsekwencji. Zmiany polityczne lub prawne mogą spowodować, że zachowania czy poglądy, które obecnie są legalne, zostaną uznane za podejrzane lub nieakceptowalne. Organy państwowe regularnie monitorują media społecznościowe i inne źródła danych, by identyfikować potencjalne zagrożenia – nawet jeśli chodzi jedynie o udział w protestach, polubienie posta czy przynależność do konkretnej grupy [19, 8, 5].

Takie zjawiska prowadzą do efektu mrożącego (chilling effect), w którym ludzie zaczynają autocenzurować się online, by uniknąć potencjalnych problemów w przyszłości. Nie chodzi już tylko o to, co użytkownik rzeczywiście zrobił, ale o to, jak dane o nim mogą zostać zinterpretowane – przez algorytmy, urzędników lub wrogie rządy [5].

6 Dobry przykład

Signal jest jednym z najbardziej znanych przykładów aplikacji zaprojektowanej z myślą o prywatności i minimalizacji danych. Firma publicznie deklaruje, że nie gromadzi nadmiarowych informacji o użytkownikach, a architektura systemu została stworzona tak, aby uniemożliwiać dostęp do treści rozmów nawet jej własnym serwerom [1, 2].

Kiedy amerykańskie służby zwróciły się do Signal z żądaniem wydania danych dotyczących określonych użytkowników, firma przekazała wszystko, co miała – i nie była w stanie dostarczyć niczego więcej. Udostępnione informacje ograniczyły się do numeru telefonu, daty rejestracji oraz daty ostatniego połączenia z serwerem. Nie było tam historii rozmów, list kontaktów, metadanych wiadomości ani żadnych innych informacji. To nie wynik zaszyfrowania danych – po prostu Signal ich nigdy nie zebrał. Ta sytuacja pokazuje, że skuteczna ochrona prywatności może wynikać nie tylko z technologii szyfrowania, ale również z decyzji projektowych ograniczających zakres przetwarzanych danych [1].

Signal angażuje się również w działania edukacyjne i uświadamiające. Przykładem może być zablokowana przez Facebooka kampania reklamowa, w której Signal chciał pokazać użytkownikom, jak szczegółowe informacje są wykorzystywane do personalizacji reklam. Reklamy te wykorzystywały dane demograficzne, zainteresowania i lokalizacje użytkowników Facebooka – dokładnie tak, jak robią to firmy reklamowe. Celem było zwrócenie uwagi na skalę inwigilacji w codziennej praktyce platform społecznościowych. Facebook zablokował kampanię, co samo w sobie stało się silnym komunikatem na temat ograniczeń przejrzystości w tych systemach [3].

Signal wyróżnia się więc nie tylko szyfrowaniem typu end-to-end, ale też konsekwentnym podejściem do prywatności, które obejmuje zarówno warstwę techniczną, jak i ideologiczną. Firma nie tylko nie może czytać wiadomości – ona po prostu nie chce wiedzieć, co robią jej użytkownicy [1, 2].

7 Podsumowanie: co robić?

Na prywatność w internecie warto patrzeć nie jako na stan zero-jedynkowy, ale jako na spektrum. Dobrym przykładem jest ilustracja z wideo Erika Murphy'ego, gdzie po jednej stronie mamy osobę, która mówi „nie mam nic do ukrycia", a po drugiej – kogoś, kto wycofał się z życia cyfrowego całkowicie [10]. Osobiście sytuuję się gdzieś na środku – "I have nothing to hide, but also nothing I want to share with you."

W codziennej komunikacji używam aplikacji takich jak Discord czy Telegram – głównie dlatego, że moi znajomi nie korzystają z bardziej prywatnych alternatyw jak Signal, Session czy SimpleX. Mam jednak pełną świadomość, że te popularne platformy nie gwarantują mi wystarczającej prywatności, dlatego celowo ograniczam im dostęp do danych, nie udzielam zbędnych uprawnień i używam ich tylko jak występuje taka potrzeba. Tematy wrażliwe zostawiam na rozmowy osobiste albo, jeśli trzeba online, to szyfrowane przy użyciu PGP jak to opisano w wideo Mental Outlaw [12].

To podejście – wybieranie narzędzi w zależności od poziomu wrażliwości tematu – to w praktyce określenie własnego modelu zagrożeń (ang. threat model). Oznacza to odpowiedzenie sobie na pytania: przed kim chcę chronić swoje dane i co dokładnie chcę chronić? Nie każdy musi się chronić przed rządem, ale każdy ma coś, co warto zachować dla siebie – niezależnie, czy to zdrowie psychiczne, życie prywatne czy prywatne relacje. Dobrze ten temat opisał Murphy [10].

Nie chodzi o to, żeby od razu „wylogować się z życia" i rzucić smartfona do rzeki. Chodzi raczej o stopniowe podejmowanie świadomych decyzji: które dane komu powierzam i z jakim ryzykiem. Nie trzeba być „paranoikiem", nie jest to zdrowe – wystarczy być świadomym i kontrolować dane, które się udostępnia.

Najważniejsze, co chcę przekazać, to: zrób tyle, ile możesz i ile ma dla Ciebie sens. Każdy krok w stronę większej prywatności jest krokiem w dobrą stronę. Nie musisz być perfekcyjny, ale jeśli świadomie unikasz powierzania wszystkiego wielkim platformom i uczysz się lepszych praktyk – to już dobrze.

Bibliografia

[1] arstechnica. „FBI demands Signal user data, but there's not much to hand over." Accessed: 2025-06-01. adr.: https://arstechnica.com/tech-policy/2016/10/fbi-demands-signal-user-data-but-theres-not-much-to-hand-over/.

[2] CEPA. „Encryption Backdoors: From Child Safety to Houthis." Accessed: 2025-06-01. adr.: https://cepa.org/article/encryption-backdoors-from-child-safety-to-houthis/.

[3] Gizmodo. „Signal Tried to Run the Most Honest Facebook Ad Campaign Ever, Immediately Gets Banned." Accessed: 2025-06-01. adr.: https://gizmodo.com/signal-tried-to-run-the-most-honest-facebook-ad-campaig-1846823457.

[4] GovTech. „There Is No Such Thing as True Privacy in the Digital Age." Accessed: 2025-06-01. adr.: https://www.govtech.com/security/there-is-no-such-thing-as-true-privacy-in-the-digital-age.html.

[5] B. C. for Justice. „Social Media Surveillance by the US Government." Accessed: 2025-06-01. adr.: https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government.

[6] M. Labs. „Amazon's Ring camera used to spy on customers." Accessed: 2025-06-01. adr.: https://www.malwarebytes.com/blog/news/2023/06/amazons-ring-camera-used-to-spy-on-customers.

[7] E. Murphy. „Can You REALLY Trust Proton Mail?" Accessed: 2025-06-01. adr.: https://www.youtube.com/watch?v=ljFAODAfAC8&t=118s.

[8] E. Murphy. „Caring about privacy almost ruined my life." Accessed: 2025-06-01. adr.: https://www.youtube.com/watch?v=Ab6ryHD_ahQ.

[9] E. Murphy. „Does Apple REALLY care about your privacy?" Accessed: 2025-06-01. adr.: https://www.youtube.com/watch?v=VgXNUuvDQ5w&t=453s.

[10] E. Murphy. „Is it impossible to be private online?" Accessed: 2025-06-01. adr.: https://www.youtube.com/watch?v=e0Qp-AOBj54.

[11] E. Murphy. „Why Do I Care So Much About Privacy?" Accessed: 2025-06-01. adr.: https://www.youtube.com/watch?v=0aXIXozAsOE.

[12] M. Outlaw. „Make ANY Messaging Service E2E Encrypted With PGP." Accessed: 2025-06-01. adr.: https://www.youtube.com/watch?v=mu2TVYJE5Gc.

[13] Plurilock. „How GDPR, CCPA, HIPAA, and Other Data Privacy Standards Safeguard Our Digital Lives." Accessed: 2025-06-01. adr.: https://plurilock.com/blog/how-gdpr-ccpa-hipaa-and-other-data-privacy-standards-safeguard-our-digital-lives/.

[14] Post-Quantum. „Harvest Now, Decrypt Later (HNDL) Risk." Accessed: 2025-06-01. adr.: https://postquantum.com/post-quantum/harvest-now-decrypt-later-hndl/.

[15] Reuters. „Tesla workers shared sensitive images recorded by customer cars." Accessed: 2025-06-01. adr.: https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[16] T. N. Y. Times. „‘Thousands of Dollars for Something I Didn’t Do’.” Archived: 2023-06-28. adr.: https://web.archive.org/web/20230628234438/https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.

[17] T. N. Y. Times. „A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal.” Archived: 2023-06-25. adr.: https://web.archive.org/web/20230625193039/https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html.

[18] T. N. Y. Times. „Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match.” Archived: 2023-06-28. adr.: https://web.archive.org/web/20230628232654/https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[19] Wired. „How Americans Are Surveilled During Protests - Uncanny Valley Podcast.” Accessed: 2025-06-01. adr.: https://www.wired.com/story/uncanny-valley-podcast-how-americans-are-surveilled-during-protests/.