

Julia Heller 
Uniwersytet Warszawski



KONTEKST, A NIE PARADOKS. JAK UŻYTKOWNICY CHRONIĄ SWOJĄ PRYWATNOŚĆ W ŚWIECIE CYFROWYM?

W artykule skupiono się na znaczeniu kontekstu w procesie decyzyjnym dotyczącym prywatności w internecie. Dotychczasowe analizy opierały się przede wszystkim na koncepcjach paradoksu prywatności, cynizmu prywatności oraz samozarządzania prywatnością, które w różny sposób wyjaśniają napięcie między deklarowanym przywiązaniem jednostki do prywatności a jej rzeczywistymi działaniami. W tekście przedstawiono wyniki badania mającego na celu sprawdzenie, czy użytkownicy zachowują się paradoksalnie w kwestii ochrony prywatności. Badanie objęło sondaż przeprowadzony wśród polskich dorosłych regularnie korzystających z internetu. Na podstawie zebranych danych wykazano, że użytkownicy nie zachowują się paradoksalnie w odniesieniu do ochrony prywatności, lecz postępują zgodnie z ramami integralności kontekstowej. Z tego powodu należy analizować kwestię dzielenia się danymi w kontekście, w którym te decyzje są podejmowane. Wyniki jasno wskazują, że użytkownicy inaczej dzielą się różnymi rodzajami danych w różnych miejscach (administrator danych) i z różnymi odbiorcami. Ponadto istnieją techniki ochrony prywatności (między innymi rozszerzenia typu „nie śledź mnie”, VPN), które powodują, że dane przestają adekwatnie odzwierciedlać rzeczywistość. Wprowadzenie pojęcia kontekstu do analizy ochrony prywatności przez użytkowników nie eliminuje asymetrii władzy, a użytkownicy nie mają możliwości zrozumienia sytuacji społecznej, jeśli nie wiedzą lub nie rozumieją, w jakim celu zbierane są ich dane.

Słowa kluczowe: prywatność; cyfrowy nadzór; integralność kontekstowa; paradoks prywatności; samozarządzanie prywatnością

Context, Not Paradox: How Do Users Protect Their Privacy in the Digital World?

The article focuses on the importance of context in the decision-making process regarding privacy on the Internet. Previous analyses have primarily been based on the concepts of the privacy paradox, privacy cynicism, and privacy self-management, which explain in different ways the tension between individuals declared attachment to privacy and their actual behaviour. The article presents the results of a study aimed at examining whether users behave paradoxically in relation to privacy protection. The study was based on a survey conducted among Polish adults who are regular Internet users. The data show

that users act according to contextual integrity regarding their privacy protection. The issue of data sharing should be analysed within the context in which these decisions are made. The findings clearly indicate that users share different types of data differently, in different places (data controllers), and with different recipients. There are privacy protection techniques (including “Do Not Track” and VPNs) that cause data to no longer adequately reflect reality. Introducing the concept of context into the analysis of users’ privacy protection does not eliminate power asymmetries. Users cannot fully understand the social situation if they do not know or understand the purposes for which their data are collected.

Key words: privacy; privacy paradox; contextual integrity; digital surveillance; privacy self-management

Wprowadzenie

Podczas korzystania z internetu użytkownicy podejmują wiele decyzji dotyczących dzielenia się swoimi danymi, na przykład czy chcą stosować narzędzia zbierające informacje o ich położeniu, mające dostęp do ich mikrofonu bądź listy kontaktów. Dodatkowo uczestnicy życia cyfrowego mogą upubliczniać choćby swój wiek, ukończone szkoły, status związku czy miejsce pochodzenia i zamieszkania. Co więcej, obecnie w zasadzie nie trzeba być aktywnym użytkownikiem internetu, aby dzielić się swoimi danymi. Nowoczesne samochody rejestrują i przesyłają informacje o stylu jazdy lub lokalizacji producentom, a nawet ubezpieczycielom. Wszystkimi tymi danymi karmią się algorytmy, które pomagają w budowaniu profili użytkowników (ustawień, preferencji i informacji o poszczególnych osobach) oraz prognozowaniu ich zachowań w określonych warunkach. Firmy komercyjne wykorzystują ten proces do zwiększenia konwersji, czyli pożądanej reakcji w ramach działań marketingowych takich jak zakup produktu, zapisanie się do newslettera czy ściągnięcie aplikacji. Pojawiają się zatem pytania: czy prywatność dla użytkowników sieci jest ważną wartością? Czy wymieniają oni dane bez żadnych ograniczeń? Te kwestie stały się inspiracją do przeprowadzenia badania na polskich regularnych użytkownikach internetu. W niniejszym artykule koncentruję się na ochronie prywatności użytkowników i użytkowniczek w internecie, rozumianej jako ograniczanie dzielenia się danymi.

Prezentowany tekst stanowi wkład do istniejącej literatury poświęconej temu zagadnieniu. Na podstawie badań empirycznych dowodzę, że użytkownicy i użytkowniczki nie zachowują się paradoksalnie w zakresie ochrony prywatności cyfrowej, lecz postępują zgodnie z ramami integralności kontekstowej. Zachowanie paradoksalne rozumiem jako niezgodności pomiędzy deklarowaniem wagi wartości prywatności a dzieleniem się danymi w internecie.

W opozycji do modelu jednostki rzekomo nieracjonalnej proponuję uwzględnić w analizie jednostkę o racjonalności włączającej kontekst jako element kalkulacji.

Rozpaczynam od omówienia podstawowych pojęć związanych z prywatnością cyfrową, kontrolą cyfrową i inwigilacją cyfrową, wykorzystując teorię integralności kontekstowej Helen Nissenbaum (2010) oraz koncepcję kapitalizmu inwigilacji Shoshany Zuboff (2020). Następnie przedstawiam najważniejsze wymiary prywatności cyfrowej oraz zarys badań nad jej ochroną w naszym kraju. W kolejnej części opisuję metodologiczne założenia badania sondażowego (CAWI) zrealizowanego na grupie dorosłych, regularnych użytkowników internetu w Polsce. Analiza wyników wykazuje rosnące stosowanie technik ochrony prywatności oraz selektywne udostępnianie danych. W dyskusji potwierdzam założenia teorii integralności kontekstowej. Kończę wnioskami, w których wskazuję, że ochronę prywatności cyfrowej należy analizować w odniesieniu do kontekstu dzielenia się danymi. Ponadto upowszechnienie technik ochrony prywatności może wpływać na funkcjonowanie całego systemu.

Prywatność cyfrowa

W literaturze przedmiotu pojęcie prywatności cyfrowej jest wyjaśniane w niejednolity sposób (Acquisti, 2004; Nissenbaum, 2010; Hull, 2015). Z tego względu analizę postawionego problemu rozpocznę od zdefiniowania kluczowych pojęć, których różne interpretacje mogą prowadzić do odmiennych wniosków badawczych.

Prywatność cyfrową ujmuję w perspektywie koncepcji integralności kontekstowej Nissenbaum: „Prawo do prywatności nie jest ani prawem do zachowania tajemnicy, ani prawem do kontroli, lecz prawem do odpowiedniego przepływu informacji osobowych”¹ (2010, s. 127). Krytykuje ona tradycyjne teorie prywatności jako zbyt sztywne. Sugeruje przy tym, że badacze nie powinni się skupiać wyłącznie na naturze samych informacji: „Bardziej zniuansowane spojrzenie na prywatność pozwala w dużym stopniu wyjaśnić, jak twierdzą sceptycy, rozbieżność zachowań i deklarowanych preferencji oraz opinii” (Martin i Nissenbaum, 2017, s. 177). Oznacza to, że troska o prywatność nie musi wykluczać gotowości do udostępniania określonych danych osobowych. Przykładowo można nie publikować w mediach społecznościowych informacji o dacie i miejscu urodzenia, a jednocześnie przystąpić do programu lojalnościowego firmy, z której usług regularnie się korzysta i której zabezpieczeniom się ufa. „Osiąganie prywatności to proces ciągły, ponieważ sytuacje społeczne nigdy nie są statyczne”

¹ Wszystkie tłumaczenia, jeśli nie zaznaczono inaczej, są mojego autorstwa (przyp. aut.).

(boyd, 2014, s. 60). Ponadto potrzeba prywatności jest wytwarzana społecznie i z tego powodu zmienia się kontekstowo i historycznie (Dopierała, 2013, s. 74). Ochrona prywatności cyfrowej zarówno w odniesieniu do innych użytkowników oraz firm technologicznych, jak i państwa nie polega na całkowitym ukrywaniu informacji, a różnorodne decyzje w tym zakresie nie dowodzą niezgodności pomiędzy deklaracjami a zachowaniem, lecz pokazują, że użytkownik działa w różnego rodzaju kontekstach.

Kontrolę cyfrową rozumiem jako działania korporacji technologicznych, instytucji państwowych oraz ośrodków badawczych, które śledzą i gromadzą dane o użytkownikach. To prowadzi do przekształcania ludzkiego życia w dane wykorzystywane następnie jako narzędzie kontroli społecznej, często bez świadomości i zgody jednostek (Zuboff, 2020, s. 83). W tym kontekście internet, który ze środka do udostępniania dokumentów przekształcił się w system organizujący i oceniający życie społeczne, coraz silniej wpływa na codzienne funkcjonowanie użytkowników. Choć zapewnia wygodę i efektywność, staje się również instrumentem kontroli i kształtowania zachowań (Fourcade i Healy, 2024, s. 32). Paradoks internetu polega na tym, że daje użytkownikom możliwość prywatnej komunikacji, a jednocześnie stwarza warunki do monitorowania i śledzenia ich aktywności przez państwa oraz firmy technologiczne (Lessig, 2006).

Utożsamiam cyfrową inwigilację ze zaktualizowanym modelem *dataveillance* (z ang. dane + inwigilacja). Joanna Strycharz i Claire Segijn rozumieją go „jako zautomatyzowane, ciągłe i (nieokreślone) gromadzenie, przechowywanie i przetwarzanie cyfrowych śladów osób lub grup za pomocą systemów danych osobowych przez podmioty państwowe i korporacyjne w celu regulowania ich zachowania lub zarządzania nim” (2022, s. 575). Badaczki zakładają, że monitorowanie i gromadzenie danych jest stałe.

Znaczenie prywatności jako wartości społecznej jest podkreślane przez fakt, że powszechnie chronią ją przepisy prawa, między innymi artykuł 12. Powszechnej Deklaracji Praw Człowieka z 1948 roku: „Nikt nie będzie podlegać arbitralnemu wkraczaniu w jego życie prywatne, rodzinę, mieszkanie lub korespondencję ani też zamachom na jego honor i reputację. Każdy jest uprawniony do ochrony prawnej przed takim wkraczaniem lub takimi zamachami” (PDPC, 1948). Wagę prywatności w środowisku cyfrowym silnie akcentują także regulacje Unii Europejskiej, takie jak dyrektywa o ePrivacy (z 2002 roku), RODO (Rozporządzenie o Ochronie Danych Osobowych z 2016 roku), akt o usługach cyfrowych (DSA z 2022 roku) czy akt w sprawie danych (Data Act z 2025 roku). Również wyniki badań empirycznych dowodzą, że prywatność jest istotną wartością dla samych użytkowników. W 2023 roku w Polsce 62% osób deklarowało większą niż pięć lat wcześniej troskę o swoją prywatność (KPMG, 2023). Liczba badanych obawiających się kradzieży danych osobowych wzrosła z 49% w 2023 roku do 64% w 2024 roku (EY, 2024). Z badania

„Polacy w social media” (IAB, 2026) wynika natomiast, że 26% badanych zrezygnowało z korzystania z mediów społecznościowych z obawy o swoją prywatność.

Po drugiej stronie znajdują się podmioty kontrolujące przepływ danych. Korporacje oraz instytucje państwowe implementują strategię ukierunkowaną na systematyczne zwiększanie liczby użytkowników oraz intensyfikację szczegółowości danych, które zostaną przez nich udostępnione. Obecność jednostki w świecie fizycznym generuje jej równoległy profil cyfrowy, stanowiący odwzorowanie tej osoby, jej gustów i aktywności, możliwych do zrekonstruowania w pełni lub częściowo z zapisów i śladów pozostawionych w systemach informacyjnych (Fourcade i Healy, 2024, s. 103). Dodatkowo komunikacja maszyna–maszyna poszerza możliwości produkcji wiedzy, czego przykładem jest internet rzeczy (ang. *Internet of Things*). Równocześnie firmy starają się utrzymać zaangażowanie użytkowników, wprowadzając elementy z gier do codziennego życia. Głównym celem wydawców i reklamodawców pozostaje wysoki poziom zaangażowania użytkowników w odbiór reklamy (Szymielewicz i Iwańska, 2019). Przykładem instytucji państwowej wykorzystującej cyfrowe ślady pozostawiane przez użytkowników jest Zakład Ubezpieczeń Społecznych, który analizuje media społecznościowe w celu weryfikacji, czy użytkownicy nie naruszają zasad korzystania ze zwolnień lekarskich (Godzieba, 2026). Marion Fourcade i Kiran Healy wskazują, że nieustanne mierzenie i klasyfikowanie stały się zasadami strukturyzującymi życie gospodarcze i społeczne. Technologia cyfrowa wprowadziła jeszcze większy poziom mierzalności życia. Autorzy pokazują, bazując na klasycznych teoriach socjologicznych (między innymi Maxa Webera, Karola Marksa, Pierre’a Bourdieu), jak rankingi, punktacja i pomiary reorganizują życie społeczne: „Społeczeństwo porządkowe tworzy porządek poprzez automatyczne rankingowanie i dopasowywanie” (Fourcade i Healy, 2024, s. 2).

Szukając odpowiedzi na pytanie, jak użytkownicy mogą chronić swoją prywatność przed cyfrową inwigilacją, opisuję zarówno podejścia zakładające pełną kontrolę jednostki nad prywatnością, jak i te, według których skuteczna ochrona wymaga zmian systemowych.

Wymiar społeczny

Jako ramę teoretyczną stosuję koncepcję integralności kontekstowej Nissenbauma. Zakłada ona, że nie można oceniać naruszeń prywatności wyłącznie na podstawie prostego podziału na informacje publiczne i prywatne (wrażliwe, intymne). Zamiast tego należy uwzględnić, że w różnych sytuacjach mogą obowiązywać odmienne normy dotyczące wielu różnych rodzajów informacji, a ich liczba jest nieograniczona (Barth i in., 2006, s. 3): „Normy zachowań wyznaczają granice akceptowalnych i nieakceptowalnych działań oraz praktyk. Niektóre

z nich definiują relacje między rolami, a tym samym kształtują struktury władzy charakterystyczne dla wielu znanych kontekstów społecznych” (Nissenbaum, 2010, s. 133). Normy te regulują przepływ danych na podstawie trzech elementów: aktorów uczestniczących w wymianie informacji (nadawcy, podmiotu, którego dotyczy informacja, i odbiorcy), typu przekazywanych informacji oraz zasad (warunków) ich transmisji (Martin i Nissenbaum, 2017, s. 190). Prywatność zostaje zachowana, gdy przepływ danych osobowych jest zgodny z normami kontekstowymi – zapewnia go integralność, poszanowanie ról i oczekiwań społecznych. Kontekst to zaś „ustrukturyzowane środowiska społeczne, charakteryzujące się kanonicznymi działaniami, rolami, relacjami, strukturami władzy, normami (lub zasadami) i wartościami wewnętrznymi (celami, zadaniami, zamierzeniami)” (Nissenbaum, 2010, s. 132). Pojęcie kontekstu od dawna jest obecne w naukach społecznych, jednak jak zauważa Teun van Dijk, badaczom trudno było zdefiniować je w sposób satysfakcjonujący (2008, s. 4). On sam proponuje teorię modeli kontekstowych, sugerując, iż „tworzenie i rozumienie tekstu oraz mówienie w sposób adekwatny i strategiczny w ujęciu ogólnym, jak również sytuacyjnym zakłada, że uczestnicy potrafią analizować, rozumieć i reprezentować sytuacje społeczne, zarówno indywidualnie, jak i zgodnie z normami grupy lub społeczności” (van Dijk 2008, s. 216). Innymi słowy, van Dijk wskazuje, że badacze powinni uwzględniać codzienne życie, doświadczenia i działania uczestników w różnych sytuacjach społecznych, aby właściwie analizować dyskurs.

Teoria integralności kontekstowej wyjaśnia przyczyny niepokoju, sprzeciwu, a czasami bierności odczuwanych wobec systemów informacyjnych tak przez specjalistów, jak przez zwykłych użytkowników. Naruszenie norm w przypadku, gdy informacje są udostępniane lub wykorzystywane w sposób niezgodny z kontekstowymi oczekiwaniami, stanowi naruszenie prywatności, określane jako zakłócenie integralności kontekstowej. Normy kontekstowe, takie jak na przykład tajemnica lekarska, odgrywają kluczową rolę: ustanawiają i podtrzymują fundamentalne praktyki społeczne oraz istotne relacje, zabezpieczają jednostki i wspólnoty przed szkodami, a także regulują rozkład władzy. Jednocześnie nie są one stałe, lecz dostosowują się do zmiennych warunków historycznych, kulturowych i geograficznych. Rozwijają się w różny sposób w poszczególnych społeczeństwach. Do podobnych wniosków doszli Martin Kovanič i Samuel Spáč, gdy badali koncepcje prywatności cyfrowej. Zauważyli współwystępowanie norm informacji kontekstowej w różnych sytuacjach prywatności, czyli w:

kontrolowanych przestrzeniach prywatnych, (dobrowolnie) współdzielonych przestrzeniach prywatnych, transakcyjnych przestrzeniach publicznych i niekontrolowanych przestrzeniach publicznych. Są one postrzegane jako odrębne konteksty nadzoru i kierują

się różnymi normami prywatności oraz różnymi oczekiwaniami jej dotyczącymi. (Kovanič i Spáč, 2022, s. 198)

Jeśli użytkownik zna cel zbierania danych, potrafi ocenić, czy ich przepływ jest zgodny z normami danego kontekstu. Gdy jednostka rozpoznaje wykroczenie poza ramy danego kontekstu, może podjąć działania ochronne, aby przywrócić zachwianą równowagę. Niemniej czasami jedyną możliwością, jaka pozostaje użytkownikowi, jest używanie starszej technologii. Dobrym przykładem są najnowsze samochody wyposażone w czujniki. Nie można już kupić nowego samochodu, który nie udostępnia danych (Kemp, 2024, s. 27).

W cyfrowym eksperymencie dotyczącym reakcji na postrzegany nadzór korporacyjny zidentyfikowano różne powody zmiany sposobu korzystania z mediów lub jej braku. Respondenci mówili o tym, że rodzaj danych ma największe znaczenie, gdy podejmują decyzję o modyfikacji swojego postępowania. Szczególną wagę przywiązują do danych, które uważają za „zbyt osobiste”. Podkreślali, że „rząd i firmy nie muszą wiedzieć o moim życiu prywatnym” oraz że zmieniliby swoje zachowanie, „gdyby otrzymywali reklamy rzeczy, o których nie chcą, żeby inni wiedzieli” (Strycharz i in., 2022, s. 9). Badano również dopasowanie teorii integralności kontekstowej do adekwatności przepływów informacji w odniesieniu do urządzeń do self-trackingu – wyniki wykazały istotny wpływ rodzaju informacji, celu jej udostępniania oraz nadawcy na postrzeganą zasadność przekazywania danych (Bourgeus i in., 2024). Jednocześnie w innych badaniach nad prywatnością „często pomijano czynniki kontekstowe, takie jak wrażliwość danych, transparentność odbiorcy [*recipient transparency* – przyp. aut.] i zasady transmisji, pomimo ich kluczowej roli w kształtowaniu obaw i zachowań związanych z prywatnością” (Herriger i in., 2025, s. 1).

Badacze piszą także o zaciemnianiu (Brunton i Nissenbaum, 2016), które działa jako forma protestu oraz oporu przeciwko wszechobecnemu nadzorowi i komercyjnemu wykorzystywaniu danych osobowych. Opór w tej koncepcji polega na celowym wprowadzeniu w błąd systemów nadzoru poprzez produkcję nieautentycznych danych oraz zniekształcanie lub ukrywanie danych przez użytkowników. Finn Brunton i Helen Nissenbaum postawili sobie za cel stworzenie metody dla drobnych graczy pozwalającej funkcjonować im w cyfrowym świecie „bez narażania się na wszechogarniającą inwigilację cyfrową” (Brunton i Nissenbaum, 2016, s. 25).

Wymiar poznawczo-behawioralny

W przeciwieństwie do koncepcji integralności kontekstowej teorie paradoksu prywatności (Acquisti, 2004; Barth i de Jong, 2017; Kokolakis, 2017) oraz cynizmu prywatności (Hoffmann i in., 2016; Segijn i Strycharz, 2025) ujmują kwestię prywatności cyfrowej całościowo, a działania użytkowników

binarnie – albo chronią oni swoją prywatność, albo tego nie robią. Z tego punktu widzenia każdy ślad cyfrowy traktowany jest jako przejaw braku dbałości o prywatność bez rozróżnienia na dane bardziej chronione i powszechnie udostępniane. Jednostki postrzegają się jako racjonalne, lecz niewystarczająco zmotywowane do ochrony prywatności. Wymienione tu teorie zakładają, że owe racjonalne jednostki wymieniają się informacjami o sobie i o swoim zachowaniu w zamian za określone korzyści. Jeśli użytkownicy deklarują, że prywatność jest dla nich ważna, a jednocześnie udostępniają swoje dane, to powstaje sprzeczność pomiędzy deklaracjami a praktykami.

Paradoks prywatności nie świadczy o tym, że ludzie są nieracjonalni. Wielu użytkowników idzie na kompromis, wybierając wygodę, podtrzymywanie więzi społecznych lub użyteczność. To prowadzi do zachowań pozornie paradoksalnych, szczególnie gdy rozpatruje się je w kontekście deklarowanych obaw (Kokolakis, 2017). Z jednej strony zakłada się, że jednostka działa racjonalnie i samodzielnie ocenia, co jest dla niej bardziej opłacalne – w tym ujęciu decyzje o udostępnianiu danych wynikają z porównania korzyści z autoprezentacji w internecie z kosztami utraty prywatności. Z drugiej strony szersza perspektywa uwzględnia społeczne uwarunkowania funkcjonowania platform internetowych. Użytkownicy czują się zobowiązani do uczestnictwa w życiu cyfrowym, aby podtrzymywać relacje społeczne. Jak ujął to Spyros Kokolakis: „należy przypuszczać, że niektóre rodzaje obaw o prywatność mają silniejszy wpływ na postawy i zachowania niż inne” (2017, s. 132).

Z kolei koncepcja cynizmu prywatności koncentruje się w większym stopniu na biernym podejściu użytkowników do nadzoru. Grzegorz Ptaszek (2019) podkreśla złożoność oraz wielowymiarowość zachowań dotyczących ochrony prywatności online, które powodują, że badacze poszukują innych wytłumaczeń niż paradoks prywatności. Świadomi nadzoru użytkownicy mają poczucie, że jako jednostki nie dadzą rady przed nim uciec. W badaniach jakościowych Segijn oraz Strycharz (2025) samo ujawnienie gromadzenia danych nie eliminuje sceptycyzmu wobec możliwości ochrony prywatności. Wręcz przeciwnie, może ono wzmacniać cynizm, jeśli praktyki nadzoru wydają się nachalne lub nieprzejrzyste. Cynizm w odniesieniu do zachowania prywatności to „postawa niepewności, bezsilności i nieufności wobec przetwarzania danych osobowych przez usługi online” (Hoffmann i in., 2016, s. 2). Zamiast wykazywać zachowania obronne, użytkownicy racjonalizują *status quo* i tolerują nadzór nad danymi, nie stawiając mu aktywnego oporu. Z czasem użytkownicy zaczynają postrzegać inwazyjne praktyki jako nieuniknioną cechę cyfrowego życia, a nie powód do krytyki lub buntu (Segijn i Strycharz, 2025). Dodatkowo niektórzy użytkownicy argumentują, że jeżeli „nie masz nic do ukrycia”, to nie trzeba się martwić nadzorem. Daniel J. Solove wskazuje, że taki argument opiera się na błędnym pojmowaniu tego, co oznacza ochrona prywatności, oraz kosztów i korzyści z niej wynikających (2011).

Wymiar systemowy

Z powodu asymetrii wiedzy i władzy użytkownicy nie mają możliwości, by skutecznie chronić swoją prywatność. Przywiązują do niej wagę i stosują techniki jej ochrony, a jednocześnie ujawniają informacje o sobie w mediach społecznościowych. Badacze podkreślają, że odpowiedzialność za ochronę prywatności została zepchnięta na jednostki, a system sprzyja wykorzystywaniu niewiedzy użytkowników lub utrudnia odmowę korzystania z usług (Hull, 2015; Zuboff, 2020). W efekcie użytkownicy nie mają pełnej kontroli nad swoim śladem cyfrowym, ponieważ to platformy dysponują znacznie szerszą wiedzą o sposobach zbierania i wykorzystywania danych.

Gordon Hull rozumie samodzielne zarządzanie prywatnością (ang. *privacy self-management*) jako kontrolę jednostki nad własnymi danymi osobowymi, wpisującą się w klasyczną tradycję ujmowania prywatności jako kontroli nad informacją o sobie (Westin, 1967; Fried, 1968). Pojęcie udanej porażki unaocznia, że „brak ochrony prywatności to tylko połowa historii. Drugą połowę stanowi ich sukces [systemów samodzielnego zarządzania prywatnością – przyp. aut.] w ustanowieniu bardzo specyficznego modelu podmiotowości etycznej” (Hull, 2015, s. 89–90). Swoje rozważania Hull opiera na późnych pracach Michela Foucaulta, który argumentował, że władza ulega internalizacji i produkuje rzeczywistość społeczną (Foucault, 2008). Zasadniczo wiedza daje ludziom zdolność do rządzenia sobą. Przykładem takiego zachowania mogą być użytkownicy wprowadzający statystykę do codziennego życia (ang. *self-tracking*) (Lupton, 2013). Praktyki te, idąc za Foucaultem, można nazwać „technologiami siebie”. Mają one na celu poprawę efektywności poprzez optymalizację funkcjonowania organizmu lub zmianę stylu życia (Wróblewski, 2016, s. 10).

Hull podkreśla, że samodzielne zarządzanie nie wystarcza do ochrony prywatności: „(1) użytkownicy nie wiedzą i nie mogą wiedzieć, na co wyrażają zgodę; (2) bardzo trudno jest wprowadzić preferencje dotyczące prywatności; (3) odmowa odwiedzania witryn naruszających prywatność staje się dla wielu osób coraz mniej realną opcją” (Hull, 2015, s. 92). Poleganie wyłącznie na samodzielnym zarządzaniu kwestią prywatności przez użytkownika okazuje się nieskuteczne i jednocześnie wzmacnia rozumienie władzy w ujęciu foucaultowskiej rządomyślności (Rose, 1999; Rose i Miller, 2017). W takim wypadku prywatność cyfrowa zostaje sprowadzona do poziomu indywidualnych decyzji o dzieleniu się danymi. Pomija się przy tym fakt, że wybory te są w dużej mierze pozorne, a prywatność ma również istotną wartość społeczną, wykraczającą poza jednostkowy rachunek zysków i strat.

Według Zuboff (2020) użytkownik z powodu głębokiej asymetrii władzy jest całkowicie pozbawiony sprawczości. Dane osobowe, wydobywane (często bez pełnej zgody użytkowników) i utowarowione przez korporacje, są

wykorzystywane do przewidywania oraz modyfikowania ludzkich zachowań. Następuje przechwytywanie, przetwarzanie i analizowanie danych użytkowników, nazywanych przez autorkę „nadwyżką behawioralną”. Jednostki nie mają możliwości obrony swojej prywatności i przeciwstawienia się dużym korporacjom technologicznym. Z perspektywy właścicieli serwisów użytkownicy są raczej zasobem niż stroną negocjującą warunki, a rzeczywistym klientem są firmy płacące za dostęp do danych, potrzebnych im do tworzenia spersonalizowanych reklam (Szymielewicz, 2016, s. 8). Temat monetyzacji danych użytkowników jest często analizowany przez badaczy społecznych. Opisują oni współczesny system gospodarczy za pomocą takich pojęć jak kapitalizm inwigilacji (Foster i McChesney, 2014; Zuboff, 2020), kapitalizm platformowy (Srniczek, 2017), iCapitalizm (Duff, 2016) czy ekonomia polubień (Gerlitz i Helmond, 2013). Podkreślają też, że wymiana w świecie cyfrowym, choć pozornie równa, tak naprawdę przyczynia się do większego wywłaszczenia użytkowników z danych. Zuboff nawet wzywa do reakcji społecznej w celu odzyskania praw do prywatności i ustanowienia przepisów chroniących jednostki przed wszechobecnym zasięgiem kapitalizmu inwigilacji. Uważa ona prywatność za podstawowe prawo człowieka, które jest niezbędne dla istnienia osobistej autonomii i demokracji. Według Zuboff odpowiedzialność za ochronę prywatności jest celowo przesuwana na jednostki, podczas gdy problem ma charakter strukturalny i systemowy. Mechanizmy „informacji i zgody” oraz „samodzielne zarządzanie prywatnością” to jej zdaniem, tak samo jak u Hulla, udane porażki. Pozornie dają kontrolę użytkownikom, ale faktycznie legitymizują wydobywanie od nich danych behawioralnych.

Z przedstawionych teorii wynika, że prywatność jest w znacznym stopniu regulowana społecznie. Zatem paradoks prywatności (Kokolakis, 2017) nie łączy się z brakiem logiki działań użytkowników, lecz z faktem, że podejmują oni decyzje w odniesieniu do norm kontekstowych obowiązujących w określonym środowisku cyfrowym (Nissenbaum, 2010). Dodatkowo dla niektórych użytkowników nie wszystkie kontekstowe elementy danej sytuacji społecznej są przejrzyste. Firmy technologiczne starają się bowiem „(...) chronić operacje zaprojektowane jako niewykrywalne, ponieważ zabierały użytkownikom bez pytania coś, co do nich należało, i wykorzystywały te arbitralnie zawłaszczone zasoby z korzyścią dla kogoś innego” (Zuboff, 2020, s. 130). W takim wypadku świadome i skuteczne chronienie swojej prywatności przez użytkowników staje się właściwie niewykonalne (Hull, 2015; Zuboff, 2020).

W niniejszym artykule staram się empirycznie udowodnić, że rozpatrywanie kwestii prywatności cyfrowej z perspektywy teorii integralności kontekstowej pozwala na pełniejsze wyjaśnienie zachowań użytkowników. Podejmuje próbę doprecyzowania pojęcia kontekstu (Nissenbaum, 2010), które umożliwia wytłumaczenie pozornie sprzecznych zachowań. Dodatkowo, bazując na

rozwiązaniach przedstawionych w książce *Zmyl trop*, eksploruję metody, dzięki którym użytkownicy mogą potencjalnie przeciwdziałać nadmiernej inwigilacji (Brunton i Nissenbaum, 2016). Tym samym wykazuję, że przypisywanie jednostce całkowitego braku sprawczości stanowi wniosek nadmiernie uogólniony (Hull, 2015; Zuboff, 2020).

Stan badań na temat prywatności polskich użytkowników internetu

Badaniem postaw polskich użytkowników wobec internetowego nadzoru – a co za tym idzie, prywatności cyfrowej – zajęła się Marta Juza (2020). Na podstawie wyników swoich badań przeprowadzonych w latach 2017 i 2019 stwierdziła, że globalne skandale dotyczące zagrożeń związanych z inwigilacją cyfrową nie przedostały się do świadomości społecznej. Jednocześnie badania Juzy pokazały, że świadomość użytkowników w kwestii gromadzenia danych przez strony internetowe jest wysoka. W 2017 roku 80% respondentów wiedziało o takiej praktyce, a w 2019 odsetek ten wzrósł do 85,3% (Juza, 2020, s. 18). Mimo rosnącej świadomości istnienia nadzoru cyfrowego towarzyszące mu obawy się nie nasiliły. Odpowiedzi respondentów dowodziły, że zdają sobie oni sprawę nie tylko z samego gromadzenia danych, lecz także z ich dalszego wykorzystywania w obrocie rynkowym oraz z generowania zysków przez podmioty zajmujące się ich przetwarzaniem. Odpowiedzi na pytania dotyczące celów zbierania danych Juza interpretuje jako „wypowiedzi charakterystyczne dla członków współczesnego społeczeństwa wraz z jego kulturą indywidualizmu” (2020, s. 19). Autorka nie dostrzegła, by świadomość nadzoru wpływała na ograniczenie skłonności do dzielenia się informacjami o sobie w internecie. Wręcz przeciwnie, użytkownicy chętnie udostępniali dane osobowe, zdjęcia oraz szczegóły ze swojego życia, w tym również informacje o charakterze intymnym. „Użytkownicy wiedzą już, że serwisy internetowe czerpią zyski z przetwarzania danych osobowych, akceptują to, doceniają zainteresowanie, śmiało dzielą się swoją prywatnością, ale oczekują w zamian jakiejś rekompensaty i innych korzyści” (Juza, 2020, s. 24).

Tematem postaw polskich użytkowników wobec moralnych aspektów prywatności w internecie zainteresował się Daniel Mider (2022). Wyniki jego badania wskazują, że 82,1% respondentów negatywnie oceniało system masowej inwigilacji o kryptonimie PRISM (tajny amerykański program szpiegowski, którego istnienie ujawnił Edward Snowden). Ponadto 62,1% uważało, że chęć pozostania anonimowym w internecie wcale nie oznacza bycia kryminalistą czy złych zamiarów. Jednocześnie jedynie 28,2% zgodziło się ze stwierdzeniem, że wygoda użytkownika stanowi wystarczającą rekompensatę za profilowanie i śledzenie przez dostawców usług. Mider, używając metody analizy skupień, wyróżnił trzy grupy użytkowników:

- grupa 1. Sceptyczni lub rozczarowani pretorianie z niskimi lub średnimi kompetencjami informatycznymi (68,7%);
- grupa 2. Umiarkowani cyberlibertarianie ze średnimi lub niskimi kompetencjami informatycznymi (21,7%);
- grupa 3. Umiarkowani lub skrajni cyberlibertarianie z wysokimi kompetencjami informatycznymi (9,6%) (Mider, 2022, s. 10).

Mider doszedł do wniosku, że polscy użytkownicy są mało skuteczni lub zupełnie nieskuteczni w ochronie swojej prywatności cyfrowej.

Nowsze badania pokazują, że polscy użytkownicy coraz lepiej dbają o prywatność cyfrową, między innymi coraz więcej osób odmawia dostępu do swojej lokalizacji geograficznej (GUS, 2021; GUS, 2023; GUS, 2024; GUS, 2025). Ponad 57% Polaków deklaruje, że zawsze dba o prywatność cyfrową (Clickmeeting, 2022). Do najczęściej stosowanych technik należą: zwracanie uwagi na pliki cookies (63,5%), dbanie o ustawienia prywatności w mediach społecznościowych (59,0%), dbanie o ustawienia prywatności w komputerze i/lub smartfonie (57,8%) (Clickmeeting, 2022).

Badania potwierdzają także, że użytkownicy odczuwają różnego rodzaju zagrożenia związane z dzieleniem się danymi. W 2021 roku najczęściej wskazywano na dwa z nich, dotyczące bezpieczeństwa danych: cyberataki i cyberprzestępczość, taką jak kradzież lub nadużycie danych osobowych, złośliwe oprogramowanie lub wyłudzenie informacji (45%) oraz wykorzystanie danych osobowych i informacji przez przedsiębiorstwa lub organy administracji publicznej (39%) (Special Eurobarometr, 2021, s. 15). Jednocześnie jedynie 35% badanych popierało monitorowanie zachowań przez służby wywiadowcze w celu zapobiegania potencjalnej przestępczości, a 37% uznało za akceptowalne stosowanie stale nasłuchujących inteligentnych asystentów. Na podstawie tych wyników można wnioskować, że Polacy wykazują raczej niechętny stosunek wobec nadzoru zarówno państwowego, jak i korporacyjnego (KPMG, 2023). W 2024 roku 49% polskich internautów zdawało sobie sprawę z działania algorytmów w mediach społecznościowych. Pozostałe 51% zakładało, że wszyscy użytkownicy serwisów społecznościowych widzą w nich te same treści, lub nie miało wiedzy bądź nie zwracało uwagi na działanie algorytmów (Miotk, 2024, s. 159). Aż 57% respondentów w Polsce uważało za dość lub bardzo prawdopodobne, że do wyświetlania reklam pozornie nawiązujących do wcześniejszych rozmów offline wykorzystywany jest podsłuch za pośrednictwem smartfona (Segijn i in., 2025). Z kolei raport NASK „Nastolatki 3.0” pokazuje, że aż 35,6% osób w wieku od 12 do 17 lat uważało, iż w internecie można pozostać całkowicie anonimowym (Lange i in., 2023, s. 102). Równocześnie z innych badań wynika, że 62% respondentów deklaruje gotowość do udostępnienia swoich danych osobowych w zamian za spersonalizowane oferty i promocje (EY, 2024).

Analiza dostępnych danych ujawnia istotne rozbieżności w wynikach. Z jednej strony badania sondażowe sugerują coraz wyższą świadomość cyfrowej inwigilacji oraz coraz większą popularność różnorodnych metod ochrony danych (Juza, 2020; Eurobarometr, 2021; Clickmeeting, 2022; GUS, 2025). Z drugiej strony widać niską skuteczność ochrony prywatności cyfrowej oraz utrzymujące się przekonanie o możliwości pozostania anonimowym w sieci (Mider, 2022; Lange i in., 2023; EY, 2024). Zarazem w danych nie widać wyraźnego skoku świadomości inwigilacji. W niniejszym artykule dążę do wyjaśnienia tych niespójności poprzez wykazanie, że to nie ogólna troska o prywatność, lecz precyzyjne zrozumienie kontekstu wykorzystania informacji determinuje intensywność i skuteczność podejmowanych działań ochronnych.

Metodologia badań

Na podstawie wcześniejszych badań prywatności polskich użytkowników (Juza, 2020; Mider, 2022) wybrałam metodę sondażową. Badanie przeprowadziłam w panelu internetowym. Zastosowałam celowo-kwotową metodę doboru próby reprezentatywną ze względu na: wiek (5), płeć (2), wykształcenie (4) i wielkość miejsca zamieszkania (7). Powodem takiej decyzji był brak operatu losowania dla populacji wszystkich internautów w Polsce. Zbiór danych został pozyskany techniką CAWI (ang. *Computer-Assisted Web Interview*) przez firmę specjalizującą się w badaniach rynku. Wykorzystanie tej techniki wynikało ze specyfiki badanej populacji, obejmującej wyłącznie osoby regularnie korzystające z internetu. Analizy przeprowadziłam na danych zebranych w Polsce na próbie $n = 1000$ dorosłych osób (18+) korzystających z internetu minimum kilka razy dziennie. Do pracy z danymi użyłam języka programowania R (R Core Team, 2025).

Dane zebrano między 25 kwietnia a 1 maja 2022 roku, a więc przed gwałtownym rozwojem sztucznej inteligencji oraz istotnymi zmianami regulacyjnymi (wprowadzeniem przez UE praw chroniących prywatność użytkowników oraz nakładających kolejne wymogi na firmy technologiczne, a także posunięciami w polityce Stanów Zjednoczonych, które miały na celu ochronę tych firm). Czynniki te mogły wpłynąć na wzrost ogólnej świadomości w zakresie inwigilacji oraz przekształcenia norm integralności kontekstowej. Warto zauważyć, że wskazywane procesy należy analizować z uwzględnieniem ich zróżnicowanej dynamiki oraz ograniczonego zasięgu oddziaływania. Owszem, rozwój sztucznej inteligencji oraz nowe regulacje prawne są istotne, jednak ich wpływ na zachowania użytkowników i świadomość społeczną nie jest ani natychmiastowy, ani powszechny. Zgodnie z teorią dyfuzji innowacji Everetta Rogersa (1983) najbardziej zaawansowane wykorzystanie nowych technologii dotyczy

głównie tak zwanych wczesnych naśladowców. Można więc założyć, że większość społeczeństwa nadal korzysta z internetu w sposób relatywnie tradycyjny, bez głębokiej renegocjacji swoich praktyk związanych z prywatnością czy świadomością w kwestii inwigilacji. Co więcej, mimo wprowadzenia przez Unię Europejską kolejnych regulacji, takich jak akt o usługach cyfrowych (DSA), ich realne przełożenie na praktykę użytkowników pozostaje wciąż niewielki ze względu na tempo ich implementacji w Polsce. W konsekwencji – choć wskazane czynniki niewątpliwie będą miały znaczenie w dłuższej perspektywie – nie ma wystarczających podstaw, by uznać, że w krótkim czasie doszło do powszechnej zmiany norm integralności kontekstowej.

Na konstrukcję mojego badania wpłynęła teoria integralności kontekstowej Nissenbaum. Jego celem była analiza różnych postaw użytkowników internetu wobec prywatności w sieci. Podjęłam następujący problem badawczy: w jaki sposób można wyjaśnić utrzymywanie się paradoksu prywatności pomimo wzrostu świadomości użytkowników na temat inwigilacji cyfrowej oraz upowszechnienia narzędzi i technik ochrony prywatności? Rozbiłam to pytanie na pytania szczegółowe, odnoszące się do poznawczych, motywacyjnych i behawioralnych aspektów postaw: (1) Jak często użytkownicy wykonują czynności chroniące prywatność cyfrową?; (2) Co skłania użytkowników do wykonywania czynności chroniących prywatność cyfrową?; (3) Czy w zeszłym roku użytkownicy udostępniali w sieci dane, na przykład w mediach społecznościowych, zakładając konto lojalnościowe, kupując online, ściągając nową aplikację mobilną?; (4) Co jest ważne dla użytkowników, gdy decydują się na udostępnianie danych w internecie? Na ich podstawie sformułowałam następujące hipotezy: (1) Osoby świadome celów wykorzystywania danych stosują więcej technik ochrony prywatności; (2) Decyzja o dzieleniu się danymi jest podejmowana w ramach różnych kontekstów.

Ułożony przeze mnie kwestionariusz zawierał 26 pytań, dotyczących między innymi sposobu korzystania z internetu (urządzenia, czynności), udostępnianych danych (miejsc, typów, częstotliwości) oraz przekonań związanych z dzieleniem się danymi. Moim zamiarem było uzyskanie informacji na temat częstotliwości oraz technik ochrony prywatności. W tym celu stworzyłam kafeterię do pytania o czynności wykonywane podczas korzystania z internetu („Jak często wykonujesz poniższe czynności, korzystając z internetu?”; odpowiedzi: „często”, „od czasu do czasu”, „nigdy nie wykonuję”). Kafeterię technik przedstawioną na wykresie 3 opracowałam na podstawie raportów (IAB, 2017; GUS, 2021), badań Marty Juzy (2020), Daniela Midera (2022) oraz książki *Zmyśl trop* Bruntona i Nissenbauma (2016). Celem analizy było opisanie praktyk związanych z ochroną prywatności cyfrowej – niezależnie od rodzaju używanego urządzenia.

Sprawdzałam również różnego rodzaju powody dzielenia się danymi. Respondenci mogli odpowiadać w pięciopunktowej skali Likerta. Dla pytania:

„Co jest dla Ciebie ważne, gdy decydujesz się na udostępnianie danych w internecie?”, przygotowałam kafeterię odpowiedzi odwołujących się do wielu motywacji (potrzeby: bezpieczeństwa, kontroli, etycznej, ekonomicznej, pragmatycznej, społecznej). Na tej podstawie stworzyłam wskaźnik kryteriów udostępniania danych. W przypadku tego wskaźnika z analizy wyłączyłam pytanie o powody społeczne („Moje dane pomagają w utrzymaniu lub poprawie jakości życia osobie, której nie znam”), ponieważ znacząco obniżało jego rzetelność. Pozostałe pozycje odnosiły się do przyczyn indywidualnych, co zapewniło większą spójność konstruktu. Po wprowadzeniu tych zmian otrzymałam wynik wskazujący na wysoką rzetelność wskaźnika (α Cronbacha = 0,81).

Pytałam też o to, dlaczego respondenci stosują techniki ograniczające dzielenie się danymi (Likert). Odwoływałam się do motywacji ekonomicznych, prawnych, chroniących intymność, nieufności instytucjonalnej czy kontroli informacji. Dzięki temu stworzyłam wskaźnik motywacji do ochrony prywatności. Wykazał on wysoką spójność wewnętrzną (α Cronbacha = 0,89).

W analizie danych ilościowych zastosowałam tabele krzyżowe. W poszukiwaniu kontekstów przeprowadziłam eksploracyjną analizę czynnikową. Do weryfikacji pierwszej hipotezy ostatecznie zastosowałam nieparametryczny test U Manna-Whitneya, a do weryfikacji drugiej hipotezy – analizę wariancji z powtarzanymi pomiarami (typ ANOVA).

Grupą, na której skupia się badanie, są regularni użytkownicy i użytkowniczki internetu z Polski. Można przypuszczać, że dla osób korzystających z internetu kilka razy dziennie lub niemal nieustannie będących online kwestia prywatności w sieci powinna stanowić istotny i świadomie analizowany aspekt codziennego funkcjonowania. W 2022 roku w Polsce 93,3% gospodarstw domowych miało w domu dostęp do internetu (GUS, 2022). Z sieci korzystały wszystkie osoby poniżej 35. roku życia, a także prawie wszystkie wśród respondentów w wieku od 35 do 44 lat. Dodatkowo 96% użytkowników internetu (tj. 74% ogółu dorosłych) korzystało z sieci bezprzewodowo (poprzez smartfon, tablet czy laptop). Obecność online co najmniej raz w tygodniu deklarowało ponad trzy czwarte dorosłych (77%), a niemal połowa ankietowanych (47%) – stałą obecność online (na bieżąco otrzymują informacje i mogą na nie reagować) (CBOS, 2022). Użytkownicy w wieku od 16 do 64 lat spędzali w internecie średnio 6 godzin i 39 minut dziennie, z czego na telefonie komórkowym 2 godziny i 58 minut, a na komputerze czy tablecie 3 godziny i 42 minuty. Pięć głównych powodów korzystania z sieci to: znajdowanie informacji, śledzenie wiadomości i aktualnych wydarzeń, sprawdzanie marek, utrzymywanie kontaktów ze znajomymi i rodziną oraz poszukiwanie nowych pomysłów i inspiracji (Datareportal, 2022).

Gdy prywatne zamienia się w widoczne

Wyniki badania potwierdzają, że użytkownicy i użytkowniczki w odmienny sposób dzielą się różnymi rodzajami danych. Pytanie o udostępnianie danych ograniczyłam do roku poprzedzającego realizację badania, aby uchwycić poziom świadomości respondentów w momencie badania oraz by zminimalizować ryzyko zniekształcenia ich pamięci po upływie zbyt długiego czasu. Na wykresie 1 widać, że respondenci różnie wyrażają zgodę na przepływ informacji. Używając eksploracyjnej analizy czynnikowej, wyodrębniłam pięć głównych wymiarów dzielenia się danymi:

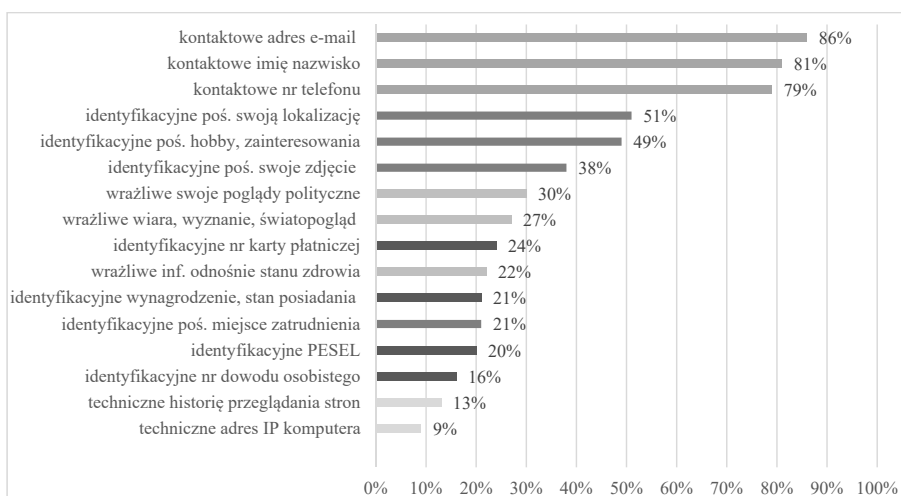
- dane wrażliwe (poglądy polityczne, wiara, wyznanie, światopogląd, informacje odnośnie stanu zdrowia) o bardzo wysokiej rzetelności omega 0,94;
- dane kontaktowe (imię nazwisko, adres e-mail, numer telefonu) o bardzo wysokiej rzetelności omega 0,96;
- dane identyfikacyjne (PESEL, numer karty płatniczej, numer dokumentu osobistego, wynagrodzenie, stan posiadania) o wysokiej rzetelności omega 0,89;
- dane identyfikacyjne pośrednie (swoje zdjęcie, swoją lokalizację, miejsce zatrudnienia, hobby, zainteresowania) o akceptowalnej rzetelności omega 0,72;
- dane techniczne (adres IP komputera, historię przeglądania stron) o akceptowalnej rzetelności omega 0,77.

W większości analizowanych kontekstów udostępniano podstawowe dane kontaktowe. W wybranych kontekstach przekazywano również dane wrażliwe oraz dane identyfikacyjne. Dane techniczne były udostępniane jedynie sporadycznie.

Na wykresie 2 przedstawiam średnią arytmetyczną skumulowanej liczby udostępnionych rodzajów danych w trzech wymiarach o najwyższej rzetelności. Użytkownicy dzielą się swoimi danymi w rozmaitych środowiskach danych i kontekstach społecznych. Wśród tych najpowszechniejszych są sklepy internetowe, media społecznościowe oraz strony instytucji publicznych. Przykładowo udostępnianie danych identyfikacyjnych na potrzeby instytucji publicznych jest generalnie akceptowane. Z kolei w mediach społecznościowych i sklepach internetowych użytkownicy najczęściej ujawniają dane kontaktowe. Wyniki widoczne na wykresie dowodzą, że użytkowników charakteryzuje selektywność względem zarówno miejsca, jak i rodzaju udostępnianych danych. Zwracanie uwagi na adekwatność przepływów informacji w kontekście (Nissenbaum, 2010), rozumiane jako umiejętność analizy, interpretacji oraz reprezentowania sytuacji społecznych (van Dijk, 2008), sprawia, że użytkownicy nie dzielą się numerem karty płatniczej czy numerem PESEL w mediach społecznościowych lub poprzez komunikatory. Jednocześnie podawanie numeru telefonu w tych kanałach nie jest dla nich problematyczne. Korporacje technologiczne mogą mieć dostęp do danych udostępnianych publicznie, jak również do treści rozmów prowadzonych z przyjaciółką za pośrednictwem komunikatora. Opinia publiczna zwróciła uwagę na

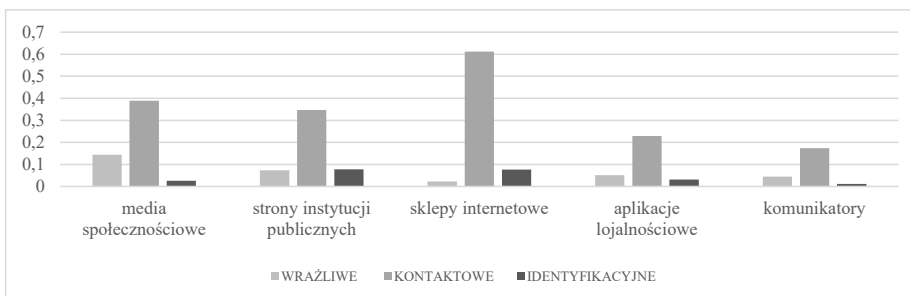
ten problem po tym, jak Edward Snowden ujawnił informacje dotyczące tajnego programu PRISM. Mimo dostępności komunikatorów zapewniających szyfrowanie end-to-end, takich jak Signal, w 2022 roku Messenger cieszył się znacznie większą popularnością (Wirtualne Media, 2022). Dopiero pod koniec 2023 roku Messenger wprowadził automatyczne szyfrowanie wiadomości.

Wykres 1. Kategorie danych udostępnianych w internecie w roku poprzedzającym badanie [pytanie: „Czy w zeszłym roku udostępniłaś(-eś) w sieci poniższe dane, na przykład w mediach społecznościowych, zakładając konto lojalnościowe, kupując online, ściągając nową aplikację mobilną?”]



Źródło: opracowanie własne.

Wykres 2. Średnia liczba udostępnianych rodzajów danych w miejscach (administrator danych) ich ujawniania



Źródło: opracowanie własne.

Ponadto, podobnie jak Juza w swoich badaniach, zapytałam użytkowników, czy wiedzą, w jaki sposób firmy wykorzystują ich dane. Jedynie 17% respondentów odpowiedziało twierdząco. Osoby te wskazały, że dane używane są w celach marketingowych („przesyłanie promocji”), do personalizacji ofert i reklam („dopasowywanie produktów do danego klienta”), tworzenia statystyk („zbiorcze, analityczne, tworzenie baz danych”) oraz na sprzedaż („Moje dane są sprzedawane natrętnym telemarketerom” [pisownia oryginalna – przyp. aut.]). Na podstawie uzyskanych wyników można stwierdzić, że wysoki poziom świadomości dotyczący gromadzenia danych przez właścicieli serwisów internetowych nie przekłada się na adekwatną wiedzę na temat sposobów ich dalszego wykorzystywania. W związku z tym nie można założyć prostej zależności przyczynowej między podstawową wiedzą a zachowaniem użytkowników.

W procesie konstruowania wskaźnika kryteriów udostępniania danych wykluczyłam pozycję odnoszącą się do motywacji społecznych. Obniżenie wskaźnika rzetelności sugerowało jej odmienny charakter względem pozostałych analizowanych czynników. Jedynie 40% respondentów wskazało, że możliwość pomocy w utrzymaniu lub poprawie jakości życia osoby, której nie znają, w dużym stopniu wpływa na ich decyzję o udostępnieniu danych. Z kolei najwięcej badanych, bo aż 86%, uznało za istotne bezpieczne zbieranie i przechowywanie danych oraz posiadanie nad nimi kontroli. W rezultacie podejście użytkowników do dzielenia się danymi można określić jako indywidualistyczne.

Wskaźnik motywacji do ochrony prywatności z wynikiem rzetelności α Cronbacha = 0,89 pokazuje w sposób konsekwentny ogólne nastawienie i wrażliwość użytkowników na tę kwestię. Jednocześnie jedynie 55% respondentów uznało za znaczące otrzymywanie dodatkowych benefitów w zamian za swoje dane (na przykład zniżki, punkty, podarunki). Wyniki te sugerują, że skłonności do dzielenia się danymi nie można wyjaśniać wyłącznie dążeniem do uzyskania dodatkowych korzyści.

Przejawem wpływu norm społecznych na podejmowanie decyzji w sprawie ochrony prywatności jest fakt, że tylko 18% respondentów przyznających, że wiedza o wykorzystywaniu danych wpływa na ich zachowanie (czyli 7% wszystkich osób biorących udział w badaniu), podaje nieprawdziwe dane. Wyraźnie dostrzegalne jest tu działanie normy prawdomówności.

Co ciekawe, 85% respondentów zgodziło się ze stwierdzeniem, że dane osobowe powinny stanowić ich własność, przy czym 54% badanych uznało, iż żadne inne podmioty nie powinny nimi dysponować. Oznacza to, że znacząca większość respondentów nadal rozumie ochronę prywatności w kategoriach kontroli i posiadania. Jednocześnie mimo silnych przekonań dotyczących własności danych użytkownicy nadal je udostępniają. Ponadto coraz częściej

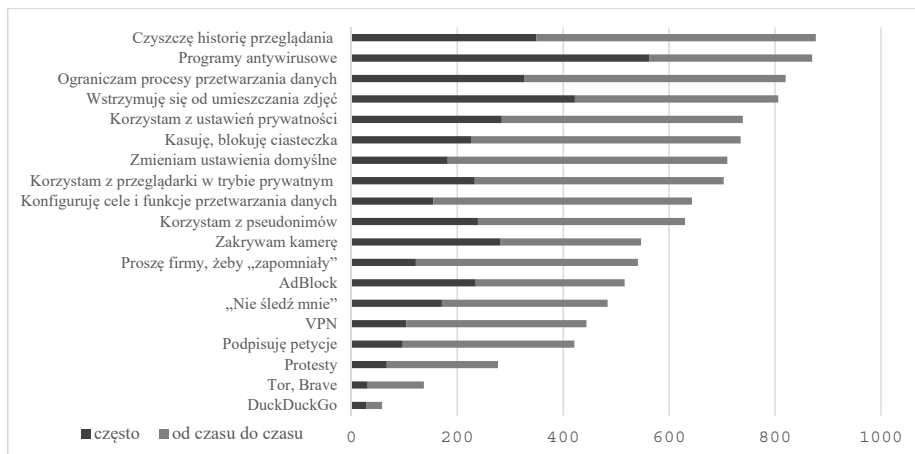
postrzegają oni swoje dane nie tylko przez pryzmat prywatności, lecz także jako zasób o wartości ekonomicznej.

Wyniki mojego badania dowodzą, że użytkownicy i użytkowniczki coraz częściej stosują metody ochrony prywatności. Podczas korzystania z internetu jedynie 1% respondentów nie wybiera żadnej z nich. Wiedza na temat sposobów wykorzystywania danych wpływa natomiast na zachowanie w internecie u 40% respondentów. Piszą oni, że starają się udostępniać jak najmniej danych („Często fałszuję dane, jeśli nie widzę sensu podawania prawdziwych”; „Nie zostawiam swoich danych w przypadkowych miejscach, bo internet traktuję jak miejsce publiczne” [pisownia oryginalna – przyp. aut.]). Uzyskane wyniki są także potwierdzeniem wniosków Juzy, zgodnie z którymi samo informowanie użytkowników o nadużyciach związanych z wykorzystywaniem zebranych danych (łamaniu norm kontekstowych – przykładami są tu choćby akta Snowdena, skandal Cambridge Analytica czy Celebgate) nie przekłada się na wzrost liczby działań chroniących prywatność.

Zapytałam respondentów także o wykorzystywane przez nich techniki ochrony prywatności (wykres 3). Niemal wszyscy sięgają po takie sposoby, jak: czyszczenie historii przeglądania, stosowanie programów antywirusowych (blokują złośliwe oprogramowanie, które umożliwia kradzież danych), ograniczanie procesów przetwarzania danych osobowych (na przykład brak zgody na wysyłanie wiadomości marketingowych) czy wstrzymywanie się od umieszczania swoich zdjęć publicznie w sieci. Techniki te stały się poniekąd standardem, ponieważ stanowią część podstawowego oprogramowania urządzeń lub wynikają z regulacji prawnych (szczególnie RODO), co sprawia, że użytkownicy mają do nich łatwy dostęp. Natomiast techniki behawioralne, takie jak podpisywanie petycji czy udział w protestach, pozostają na marginesie praktyk użytkowników. Wyniki (wykres 3) uprawniają do wniosku, że użytkownicy preferują indywidualne i bardziej pasywne rozwiązania techniczne niż aktywne działania kolektywne. Używanie bardziej niszowych narzędzi, takich jak DuckDuckGo, Tor, Brave czy VPN, również jest mniej popularne.

Jednym z elementów wpływających na możliwości ochrony prywatności przez użytkowników jest prawo. W 2018 roku w całej Unii Europejskiej weszło w życie RODO. W skrócie – miało ono zapewnić osobom fizycznym większą kontrolę nad ich danymi osobowymi. Zapytałam respondentów, czy uważają, że rzeczywiście tak się stało. Mniej niż połowa (46%) odpowiedziała twierdząco. Jednocześnie znacząca większość (84%) ograniczała procesy przetwarzania swoich danych osobowych (na przykład brak zgody na wysyłanie wiadomości marketingowych), a ponad połowa (54%) skorzystała z prawa do żądania usunięcia swoich danych osobowych i zaprzestania dalszego ich przetwarzania. Obie te opcje zostały wprowadzone przez RODO.

Wykres 3. Techniki ochrony prywatności



Źródło: opracowanie własne.

Ponadto przeprowadziłam weryfikację postawionych hipotez badawczych, wykorzystując zaawansowane techniki statystyczne dopasowane do charakteru zgromadzonych danych. W celu doboru odpowiedniego aparatu statystycznego do weryfikacji pierwszej hipotezy – zakładającej, że osoby świadome celów wykorzystywania danych stosują więcej technik ochrony prywatności – sprawdziłam normalność rozkładu zmiennych w obu grupach (osób deklarujących wiedzę na temat celów wykorzystywania ich danych oraz osób takiej wiedzy nieposiadających) za pomocą testu Shapiro-Wilka. Ponieważ oba wyniki pokazały istotne odstępstwo od rozkładu normalnego ($p < 0,05$), do weryfikacji hipotezy ostatecznie zastosowałam nieparametryczny test U Manna-Whitneya. Asymetria wynikała z odpowiedzi respondentów – aż 83% badanych zadeklarowało, że nie wie, do jakich celów firmy wykorzystują ich dane. Tym samym hipoteza pierwsza została potwierdzona. Przeprowadzona analiza wykazała istotne statystycznie różnice między badanymi grupami ($U = 57214$; $p < 0,001$). Osoby deklarujące wiedzę na temat celów, do których firmy wykorzystują ich dane, stosują znacznie więcej technik ochrony. Wyniki te wskazują nie tyle na kwestię świadomości faktu zbierania danych, ale rozumienie, w jaki sposób są one przetwarzane. Wiedza na ten temat może pomóc w wyborze adekwatnych metod ochrony prywatności.

W celu weryfikacji drugiej hipotezy, dotyczącej kontekstowego charakteru udostępniania danych, zastosowałam analizę wariancji z powtarzanymi pomiarami (typ ANOVA). Wybór tego testu był podyktowany czterema grupami oraz założeniem, że ten sam użytkownik zachowuje się inaczej w różnych sytuacjach. Analiza potwierdziła, że kontekst (miejsce) ma statystycznie istotny wpływ na

skłonność do dzielenia się danymi we wszystkich badanych wymiarach. Wyniki te sugerują, że użytkownicy nie traktują prywatności zero-jedynkowo. Mają raczej zróżnicowane podejścia, zależne od typu udostępnianych danych, co podważa stosowanie uproszczonego modelu „wszystko albo nic” w badaniach nad prywatnością cyfrową.

Tabela 1. Wyniki analizy ANOVA

Wymiar danych	Statystyka F	Istotność p	Wielkość efektu (η^2)
Wrażliwe	F(4,3996) = 70,93	p < 0,001	0,05
Kontaktowe	F(4,3996) = 260,46	p < 0,001	0,14
Identyfikacyjne	F(4,3996) = 114,56	p < 0,001	0,08
Identyfikacyjne pośrednie	F(4,3996) = 212,52	p < 0,001	0,14
Techniczne	F(4,3996) = 12,44	p < 0,001	0,01

Źródło: opracowanie własne.

Podsumowując, moje badania – w odróżnieniu od wyników badań Juzy, mówiących o wysokiej świadomości nadzoru przy jednocześnie niskiej skłonności do ograniczania dzielenia się danymi – pokazują rosnące wykorzystanie technik ochrony prywatności cyfrowej. Ponadto niewiele ponad połowa respondentów uznaje otrzymanie jakiejś rekompensaty za ważny czynnik wpływający na decyzję o udostępnianiu danych, co nie pokrywa się z wnioskami przedstawionymi przez Juzę. Może to świadczyć o rosnącej świadomości użytkowników w zakresie zagrożeń wynikających z dzielenia się danymi. Uzyskane wyniki dowodzą również, że dane są udostępniane selektywnie. Rozkład decyzji dotyczących udostępniania danych różni się istotnie statystycznie w zależności od kontekstu. Respondenci deklarują też, że dane powinny należeć do nich, co odzwierciedla ideę prawa do odpowiedniego przepływu informacji, a nie jedynie prawa do tajemnicy czy kontroli. Choć stosowanie przez użytkowników internetu coraz większej liczby technik ochrony prywatności może sugerować wzrost ich kompetencji i świadomości, to równocześnie ujawnia napięcie między deklarowaną przez nich troską o dane a strukturalnymi ograniczeniami, które podważają skuteczność jednostkowych działań.

Dyskusja

Prywatność cyfrowa i podejście użytkowników do jej ochrony staje się coraz częściej podejmowanym tematem w naukach społecznych, a mimo to jako badacze nie potrafimy wytłumaczyć wielu zaobserwowanych fenomenów. Można stwierdzić za Kokolakisem, że „choć przeprowadzono wiele badań

nad paradoksem prywatności, pozostaje on szeroko otwartym zagadnieniem” (Kokolakis, 2017, s. 132). Wskazuje on na problem rozpatrywania tego fenomenu w izolacji. Moje badania częściowo starają się uniknąć tego błędu, gdyż biorą pod uwagę nie tylko społeczno-demograficzne charakterystyki respondentów, ale także sposoby użytkowania internetu, praktyki dzielenia się danymi, jak również przekonania ich dotyczące.

Potwierdzenie pierwszej hipotezy daje podstawę do częściowej polemiki z tezami Zuboff. Twierdzi ona, że użytkownik nie ma mocy do przeciwstawiania się systemowi. Wyniki mojego badania sugerują jednak, że świadomość mechanizmów przetwarzania danych może częściowo redukować skutki asymetrii wiedzy i władzy. Choć całkowite zachowanie anonimowości w sieci jest praktycznie niemożliwe, istnieją sposoby ograniczania dzielenia się danymi lub podawania nieprawdziwych danych. Minimalizowanie przepływu wiarygodnych danych zauważalnie utrudnia pracę algorytmów. Celem firm komercyjnych jest wykorzystanie działań marketingowych do zwiększania sprzedaży i w konsekwencji generowania zysku. Jeśli dane używane w działaniach marketingowych będą niepełne lub nieprawidłowe, osiągnięcie tego celu stanie się droższe. Jednocześnie niedostateczne rozpowszechnienie wiedzy na temat mechanizmów przetwarzania danych częściowo potwierdza diagnozę Zuboff. Pojedynczy użytkownik nie jest w stanie znacząco zaburzyć funkcjonowania systemu, niemniej skala takich przypadków może wpływać na jego efektywność. System działa właśnie dlatego, że większość użytkowników nie ma pełnego wglądu w sposoby gromadzenia i wykorzystywania danych. Z tego powodu regulaminy i warunki korzystania z usług są często pisane skomplikowanym językiem prawniczym, ustawienia prywatności w większości są ukryte, a proces zarządzania nimi jest czasochłonny i utrudniony.

Na zachowania chroniące prywatność można też patrzeć w kategoriach oporu wobec cyfrowej inwigilacji. Brunton i Nissenbaum poświęcają rozdział swojej książki kwestiom etycznym związanym z zaciemnianiem. Jednym z zarzutów wobec tej formy ochrony prywatności było oskarżenie o nieuczciwość. Autorzy bronią się stwierdzeniem, że „zaciemnianie jest oporem przeciwko przymusowi, wyzyskowi albo groźbom” (Brunton i Nissenbaum, 2016, s. 158). Natomiast w ramach integralności kontekstowej opór to wskaźnik sygnalizujący naruszenia w przepływie informacji osobistych w określonym kontekście. Nissenbaum wyróżnia różne formy działań oporowych: indywidualne i pasywne, takie jak „zrezygnowane narzekania jednostek”, zbiorowe i aktywne, czyli „głośne protesty grup interesu i elokwentnych polityków”, a także instytucjonalne i eksperckie, obejmujące „naukowe publikacje i [publikacje – przyp. aut.] w mediach popularnych” (Nissenbaum, 2010, s. 1). Nawet jeżeli użytkownicy częściej wybierają indywidualne, pasywne rozwiązania techniczne niż aktywne działania zbiorowe, wciąż można uznać je za techniki oporu.

W niniejszym artykule jasno argumentuję, że kwestii ochrony prywatności nie powinno się analizować w sposób binarny. Podczas korzystania z sieci użytkownicy podejmują wiele decyzji dotyczących dzielenia się danymi. Wynik analizy ANOVA stanowi bezpośrednie, empiryczne potwierdzenie koncepcji integralności kontekstowej (Nissenbaum, 2010). Nissenbaum zakłada, że prywatność nie polega na prostym ukrywaniu informacji, lecz na odpowiednim przepływie danych w zależności od kontekstu społecznego. Moje badania udowadniają, że zamiast z prostym „paradoksem” mamy do czynienia z racjonalnością uwarunkowaną kontekstowo. Na kwestię prywatności należy patrzeć przez pryzmat kontekstu, w którym zapadają decyzje o dzieleniu się danymi. Ponadto koncepcje takie jak paradoks prywatności, cynizm prywatności czy teoria udanej porażki opierają się na błędnym przekonaniu, że każda decyzja o udostępnieniu danych ma dla użytkownika taką samą wagę. Badania na polskich użytkownikach wyraźnie pokazują, że coraz więcej osób korzysta z metod ochrony prywatności, jednocześnie nie rezygnując z dzielenia się danymi. Zgodnie z teorią paradoksu prywatności zachowania te powinny się wzajemnie wykluczać, jednak moje badania podkreślają zróżnicowaną wagę przypisywaną poszczególnym rodzajom danych w odmiennych kontekstach (wykres 2).

Przestrzeganie norm kontekstowych może się również zmieniać w czasie. Wskazuje na to między innymi zachowanie dotyczące umieszczania swoich zdjęć w sieci. Coraz więcej użytkowników powstrzymuje się od takich działań (w 2022 roku – 42% często i 38% od czasu do czasu; IAB w 2016 roku – 47% od czasu do czasu). Przykład ten unaocznia, że użytkownicy potrafią przynajmniej częściowo zmniejszyć skalę dzielenia się swoim życiem online. Takie zachowanie pozostaje w sprzeczności ze stwierdzeniem, że nie istnieje realna możliwość odmowy korzystania z witryn naruszających prywatność (Hull, 2015). Na normy społeczne mogą wpływać także zmiany prawne w innych krajach, czego ilustracją jest kwestia ograniczania dostępu najmłodszych do mediów społecznościowych w Polsce (Strzełińska, 2026). Pod tym względem przykład RODO, które można rozpatrywać w kategoriach udanej porażki (Hull, 2015; Zuboff, 2020), pokazuje, że oddziaływanie regulacji prawnych na normy społeczne może okazywać się większe niż ich bezpośrednia skuteczność w zakresie ochrony praw użytkowników. Z jednej strony użytkownicy nie widzą poprawy, jeśli chodzi o kontrolę nad swoimi danymi, a z drugiej – robią użytek z możliwości, które wprowadziło to rozporządzenie.

Zdecydowana większość respondentów uważa, że dane osobowe powinny stanowić ich własność. Stanowisko to koresponduje z neoliberalną logiką uwarowienia danych osobowych krytykowaną przez Zuboff (2020). Takie podejście paradoksalnie ułatwia rozwój kapitalizmu inwigilacji poprzez ujmowanie prywatności w kategoriach własnościowych, a nie jako prawa społecznego. Gdyby jednak w analizie wyników przyjąć perspektywę binarną, uwypuklone

zostałoby zjawisko paradoksu prywatności (Kokolakis, 2017). Inaczej wyniki te można interpretować w ramach podejścia kontekstowego Nissenbaum (2010). Wówczas wskazują one na napięcie pomiędzy abstrakcyjnymi zasadami a praktykami zależnymi od kontekstu. Użytkownicy mogą deklarować chęć absolutnej własności danych, w praktyce akceptując ich przepływ w określonych kontekstach społecznych.

Ograniczenia i przyszłe badania

Moje badanie dowodzi, że kontekst odgrywa kluczową rolę w podejmowaniu decyzji o udostępnianiu danych, niemniej wyniki opierają się na próbie pochodzącej z jednego kraju i określonego momentu. Nie dają podstaw do generalizacji i nie można przenosić ich na światową populację użytkowników i użytkowników internetu.

Wyniki badania sondażowego dzięki przedstawieniu zestawu deklarowanych zachowań respondentów nakierowały moją uwagę na praktyczne znaczenie kontekstu w kwestii ochrony prywatności. Tego rodzaju badania mają jednak swoje ograniczenia: „Sondaże nie mogą mierzyć działań społecznych. Mogą one jedynie gromadzić relacje badanych o ich przeszłych działaniach” (Babbie, 2003, s. 302). Z powodu możliwości używania tylko uogólnionych pytań i abstrakcyjnych scenariuszy, oderwanych od konkretnych decyzji respondentów, trudno uchwycić kontekst działań, które podejmują oni, aby chronić swoją prywatność. W przypadku złożonych problemów społecznych przydatne staje się łączenie różnych podejść teoretycznych, żeby analizować konteksty i odnosić je do wypowiedzi badanych (Wodak, 2011). By uzyskać wgląd w proces decyzyjny jednostki, konieczne jest odnalezienie równowagi między wartościami indywidualnymi a wartościami społecznymi prywatności.

W przyszłych projektach można rozszerzyć badania o inne kraje, aby sprawdzić działanie różnego rodzaju norm społecznych. Przykładowo wskaźniki akceptowalności personalizacji algorytmicznej i wykorzystania danych osobowych w internecie znacząco różnią się w Stanach Zjednoczonych i w Niemczech (Kozyreva i in., 2021). Dodatkowo badacze powinni używać triangulacji metodologicznej. Dla uchwycenia pełnego kontekstu zachowań użytkowników proponuję zrealizowanie badań jakościowych. Przeprowadzenie wywiadów grupowych pozwoli uczestnikom skonfrontować własne wyobrażenia dotyczące prywatności w trakcie dyskusji. Połączenie różnych wymiarów (świadomości, kompetencji, motywacji i norm) umożliwi lepsze zrozumienie złożonej dynamiki działań użytkowników w zakresie ochrony prywatności cyfrowej.

Wnioski

Przedstawiane tutaj wyniki badania można podsumować w trzech najważniejszych punktach. Po pierwsze, badania nad prywatnością powinny uwzględniać kontekst. Analizy opisujące tak zwany paradoks prywatności opierają się na nieuprawnionym założeniu, że jednostka deklarująca, iż prywatność jest dla niej ważną wartością, za każdym razem konsekwentnie będzie ją chronić (nie udostępniać danych). Zgromadzone przeze mnie dane przeczą tezie, że użytkownicy podchodzą binarnie do tematu ochrony prywatności. Nie stosują oni uniwersalnych zasad ochrony, lecz kontekstowo różnicują swoje działania, dopasowując je do norm społecznych. Potwierdza to koncepcję Nissenbaum, która pisze, że „choć autoprezentacja jest ważnym powodem, aby wspierać kontrolę podmiotów nad informacjami osobistymi, istnieją ważne konteksty, w których (...) musi ona ustąpić miejsca alternatywnym zasadom przekazywania informacji” (2010, s. 178). Ponadto Nissenbaum uważa, że troszcząc się o prywatność, można dzielić się swoimi danymi, dopóki nie wykracza się poza ramy norm kontekstowych. W konsekwencji użytkownicy nie zachowują się paradoksalnie, lecz postępują zgodnie z zasadami integralności kontekstowej.

Po drugie, na podstawie wyników badań sondażowych częściowo zidentyfikowałam kontekst podejmowania decyzji dotyczących ochrony prywatności lub jej braku. Jednoznacznie wskazują one, że zarówno rodzaj danych, jak i miejsce ich udostępniania wpływają na zachowania użytkowników. Wykazałam również oddziaływanie norm społecznych na wybór sposobu ochrony prywatności. Norma prawdomówności zdaje się silniejsza niż możliwość chronienia swojej prywatności przy użyciu technik zaciemniania. Ponadto zauważyłam, że świadomość celu wykorzystywania danych częściowo rzutuje na działania użytkowników w sieci. Bourgeus, Vandercruysse i Verhulst także potwierdzili, że cel udostępniania informacji (zwłaszcza reklamowy) ma istotne znaczenie przy ocenianiu odpowiedniości dzielenia się danymi (2024, s. 7). Porównywalnie do koncepcji cynizmu prywatności (Segijn i Strycharz, 2025) moje badania dowodzą, że sama świadomość nadzoru nie wystarczy do tego, aby użytkownicy konsekwentnie chronili swoją prywatność. Dodatkowo analiza odpowiedzi respondentów pokazała, że większość użytkowników nie wie, do czego firmy wykorzystują ich dane. W tym kontekście nakaz informowania użytkowników o celu zbierania danych wprowadzony przez RODO jest najwyraźniej niewystarczający.

Po trzecie, polemizuję z założeniem Zuboff, zgodnie z którym nadwyżka behawioralna powstaje na bazie prawdziwej aktywności człowieka. Badaczka twierdzi, że „opór użytkownika nie będzie przeszkodą w wywłaszczeniu danych. Żadne ograniczenia moralne, prawne i społeczne nie staną na drodze poszukiwania, zawłaszczania i analizowania zachowań innych ludzi w celach

komercyjnych” (Zuboff, 2020, s. 117). Jednak gdy użytkownicy stosują rozszerzenia do przeglądarek, takie jak TrackMeNot czy Don't Track Me Google, podają nieprawdziwe dane, używają VPN (szyfrując tym samym ruch internetowy i maskując rzeczywisty adres IP) lub korzystają z pseudonimów, dane przedstawiają adekwatnie odzwierciedlać rzeczywistość. Obecnie margines błędu może nie osiągać poziomu istotności statystycznej, ale takie praktyki mogą prowadzić do obniżenia wydolności systemu. Na podobną kwestię zwraca uwagę José van Dijk, kiedy dekonstruuje ideologiczne podstawy datafikacji oraz dataizmu: „entuzjaści datafikacji często zakładają oczywisty związek między danymi a ludźmi” (van Dijk, 2014, s. 199).

Problematyka prywatności wykracza poza proste napięcie między deklarowanym przywiązaniem do tej wartości a realnymi działaniami jednostek. Wprowadzenie pojęcia kontekstu do analizy ochrony prywatności przez użytkowników nie eliminuje asymetrii władzy ani mechanizmów jej wykorzystywania do coraz większego wywłaszczania użytkowników (Zuboff, 2020). Opierając się na teorii modeli kontekstowych (van Dijk, 2008), stwierdzam, że w momentach podejmowania przez użytkowników decyzji o dzieleniu się danymi często występuje naruszenie kontekstowych norm społecznych, ponieważ nie mają oni możliwości zrozumienia sytuacji społecznej, kiedy nie wiedzą lub nie rozumieją, w jakim celu gromadzone są ich dane. Ma to szczególne znaczenie, ponieważ znajomość celu wykorzystywania danych wpływa na decyzje użytkowników (Bourgeus i in., 2024).

Finansowanie

Badania zostały sfinansowane przez Uniwersytet Warszawski w ramach programu „Inicjatywa Doskonałości – Uczelnia Badawcza (2020–2026)”.

Podziękowania

Chciałabym serdecznie podziękować mojemu Promotorowi, dr hab. Mikołajowi Lewickiemu, za wsparcie merytoryczne, cenne wskazówki oraz opiekę naukową na każdym etapie pracy. Szczególne podziękowania składam również Recenzentom za poświęcony czas, uważną lekturę oraz wartościowe uwagi, które przyczyniły się do podniesienia jakości niniejszego artykułu. Wyrazy wdzięczności kieruję także do mojej Mamy za pomoc w redakcji tekstu. Dziękuję także grupie doktorantów za celne komentarze, konstruktywne dyskusje oraz inspirujące sugestie.

Bibliografia

- Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. *Proceedings of the ACM Conference on Electronic Commerce*, 21–29.
- Babbie, E. (2003). *Badania społeczne w praktyce* (F. Tyl, tłum.). PWN.
- Barth, A., Datta, A., Mitchell, J. C., Nissenbaum, H. (2006). Privacy and Contextual Integrity: Framework and Applications, *IEEE Symposium on Security and Privacy*. <https://doi.org/10.1109/SP.2006.32>
- Barth, S., de Jong, M. D. T. (2017). The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review. *Telematics and Informatics*, 34(7). <https://dx.doi.org/10.1016/j.tele.2017.04.013>
- Bourgeois, A., Vandercruysse, L., Verhulst, N. (2024). Understanding Contextual Expectations for Sharing Wearables' Data: Insights From a Vignette Study. *Computers in Human Behavior Reports*, 15, 100443. <https://doi.org/10.1016/j.chbr.2024.100443>
- boyd, d. (2014). *It's Complicated: The Social Lives of Networked Teens*. Yale University Press.
- Brunton, F., Nissenbaum, H. (2016). *Zmył trop. Na barykadach prywatności w sieci. Przewodnik* (J. Konieczny, tłum.). PWN.
- Dopierała, R. (2013). *Prywatność w perspektywie zmiany społecznej*. Nomos.
- Duff, A. (2016). Rating the Revolution: Silicon Valley in Normative Perspective. *Information, Communication & Society*, 19(11), 1605–1621. <https://doi.org/10.1080/1369118X.2016.1142594>
- Foster, J., McChesney, R. (2014). Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age. *Monthly Review*, 66(3). https://doi.org/10.14452/MR-066-03-2014-07_1
- Foucault, M. (2008). *The Birth of Biopolitics. Lectures at the Collège de France, 1978–79* (M. Senellart, red.). Palgrave MacMillan.
- Fourcade, M., Healy, K. (2024). *The Ordinal Society*. Harvard University Press.
- Fried, C. (1968). Privacy. *Yale Law Journal*, 77(3), 475–493.
- Gerlitz, C., Helmond, A. (2013). The Like Economy: Social Buttons and the Data-Intensive Web. *New Media & Society*, 15(8), 1348–1365. <https://doi.org/10.1177/1461444812472322>
- Godzieba, M. (2026). ZUS monitoruje media społecznościowe podczas L4. Co warto wiedzieć. <https://www.onet.pl/styl-zycia/kbpl-2/zus-monitoruje-media-spolecznosciowe-podczas-l4-co-warto-wiedziec/kx2zf2g,0666d3f1> [dostęp: 30.07.2026].
- Herriger, C., Merlo, O., Eisingerich, A. B., Arigayota, A. R. (2025). Context-Contingent Privacy Concerns and Exploration of the Privacy Paradox in the Age of AI, Augmented Reality, Big Data, and the Internet of Things: Systematic Review. *Journal of Medical Internet Research*, 27(7), e71951. <https://doi.org/10.2196/71951>
- Hoffmann, C. P., Lutz, C., Ranzini, G. (2016). Privacy Cynicism: A New Approach to the Privacy Paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4). <https://doi.org/10.5817/CP2016-4-7>

- Hull, G. (2015). Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data. *Ethics and Information Technology*, 17(2), 89–101. <https://doi.org/10.1007/s10676-015-9363-z>
- Juza, M. (2020). Postawy polskich użytkowników Internetu względem nadzoru obecnego w sieci. *Studia Humanistyczne AGH*, 19(1), 7–26. <https://doi.org/10.7494/human.2020.19.1.7>
- Kemp, K. (2024). *Driving Blind: The Unexamined Privacy Risks of Connected Cars*. UNSW Sydney.
- Kokolakis, S. (2017). Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. *Computers & Security*, 64, 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>
- Kovanič, M., Spáč, S. (2022). Conceptions of Privacy in the Digital Era: Perceptions of Slovak Citizens. *Surveillance & Society*, 20(2), 186–201. <https://doi.org/10.24908/ss.v20i2.14099>
- Kozyreva, A., Lorenz-Spreen, P., Hertwig, R. (2021). Public Attitudes Towards Algorithmic Personalization and Use of Personal Data Online: Evidence from Germany, Great Britain, and the United States. *Humanities and Social Sciences Communications*, 8. <https://doi.org/10.1057/s41599-021-00787-w>
- Lessig, L. (2006). *Code Version 2.0*. Basic Books.
- Lupton, D. (2013). Quantifying the Body: Monitoring and Measuring Health in the Age of mHealth Technologies. *Critical Public Health*, 23, 393–403. <http://dx.doi.org/10.1080/09581596.2013.794931>
- Martin, K., Nissenbaum, H. (2017). Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables. *Science & Technology Law Review*, 18(1), 176–218. <https://doi.org/10.7916/stlr.v18i1.4015>
- Mider, D. (2022). Privacy on the Internet: An Empirical Study of Poles' Attitudes. *Applied Cybersecurity & Internet Governance*, 1(1), 208–223. <https://doi.org/10.5604/01.3001.0016.1459>
- Miotk, A. (2024). *Świadomość algorytmiczna a ewolucja widowni*. Wydawnictwo Naukowe i Edukacyjne Stowarzyszenia Bibliotekarzy Polskich.
- Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford University Press.
- Ptaszek, G. (2019). *Edukacja medialna 3.0 Krytyczne rozumienie mediów cyfrowych w dobie Big Data i algorytmizacji*. Wydawnictwo UJ.
- R Core Team. (2025). R: A Language and Environment for Statistical Computing. R. Foundation for Statistical Computing. <https://www.R-project.org> [dostęp: 30.07.2026].
- Rogers, E. (1983). *Diffusion of Innovations*. The Free Press.
- Rose, N. (1999). *Powers of Freedom*. Cambridge University Press.
- Rose, N., Miller, P. (2017). Political Power Beyond the State: Problematics of Government. W: P. Fitzpatrick (red.), *Foucault and Law* (s. 191–223). Routledge.
- Segijn, C. M., Strycharz, J. (2025). Transparency, Awareness, and Privacy Cynicism: Exploring Appropriate Dataveillance for Personalized Advertising Through Qualitative Interviews. *Journal of Interactive Advertising*, 25(3), 272–284. <https://doi.org/10.1080/15252019.2025.2546338>

- Segijn, C. M., Strycharz, J., Turner, A., Oprea, S. J. (2025). "My Phone Must be Listening!": Peoples' Surveillance Beliefs Around Devices "Listening" to Offline Conversations in the US, the Netherlands, and Poland. *Big Data & Society*, 12(2). <https://doi.org/10.1177/20539517251337102>
- Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security*. Yale University Press.
- Srnicek, N. (2017). *Platform Capitalism*. Polity Press.
- Strycharz, J., Segijn, C. M. (2022). The Future of Dataveillance in Advertising Theory and Practice. *Journal of Advertising*, 51(5), 574–591. <https://doi.org/10.1080/00913367.2022.2109781>
- Strycharz, J., Kim, E., Segijn, C. (2022). Why People Would (Not) Change Their Media Use in Response to Perceived Corporate Surveillance. *Telematics and Informatics*, 71, 101838. <https://doi.org/10.1016/j.tele.2022.101838>
- Strzełińska, K. (2026). Zakaz social mediów dla dzieci w Polsce? Wyniki sondażu CBOS dla DGP. <https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/10644-741,polacy-chca-ograniczyc-dzieciom-dostep-do-social-mediow-sondaz-dgp.html> [dostęp: 30.07.2026].
- Szymielewicz, K. (2016). Słowo wstępne. Jeszcze możemy odzyskać kontrolę. W: F. Brunton, H. Nissenbaum, *Zmył trop. Na barykadach prywatności w sieci*. Przewodnik (s. 5–18). PWN.
- Szymielewicz, K., Iwańska, K. (2019). *Śledzenie i profilowanie w sieci*. Fundacja Panoptikon.
- van Dijck, J. (2014). Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology. *Surveillance & Society*, 12(2), 197–208. <https://doi.org/10.24908/ss.v12i2.4776>
- van Dijk, T. (2008). *Discourse and Context. A Sociocognitive Approach*. Cambridge University Press.
- Westin, A. (1967). *Privacy And Freedom*. Athenum.
- Wodak, R. (2011). Wstęp. Badania nad dyskursem – ważne pojęcia i terminy. W: R. Wodak, M. Krzyżanowski (red.), *Jakościowa analiza dyskursu w naukach społecznych* (D. Przepiórkowska, tłum.). Oficyna Wydawnicza ŁośGraf, 11–37.
- Wróblewski, M. (2016). Nowe szaty healthismu. Self-tracking, neoliberalizm i kapitalizm kognitywny. *Acta Universitatis Lodziensis. Folia Sociologica*, 58, 5–23. <https://doi.org/10.18778/0208-600X.58.01>
- Zuboff, S. (2020). *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy* (A. Unterschuetz, tłum.). Zys i S-ka.

Raporty

- CBOS. (2022). Korzystanie z internetu w 2022 roku. https://www.cbos.pl/SPISKOM.POL/2022/K_077_22.PDF [dostęp: 30.07.2026].
- Clickmeeting. (2022). Prywatność online. Opinie użytkowników i dobre praktyki. <https://knowledge.clickmeeting.com/uploads/2022/03/ClickMeeting-Prywatność-online.-Opinie-użytkowników-i-dobre-praktyki-PL.pdf> [dostęp: 30.07.2026].

- Datareportal. (2022). Digital 2022 Poland. <https://datareportal.com/reports/digital-2022-poland> [dostęp: 30.07.2026].
- EY. (2024). Future Consumer Index. https://www.ey.com/pl_pl/newsroom/2024/12/ey_future_consumer_index_cyber_polska [dostęp: 30.07.2026].
- GUS. (2021). Społeczeństwo informacyjne w Polsce w 2021 r. https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/2/11/1/spoleczenstwo_informacyjne_w_polsce_w_2021_r..pdf [dostęp: 30.07.2026].
- GUS. (2022). Społeczeństwo informacyjne w Polsce w 2022 r. <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2022-roku,1,16.html> [dostęp: 30.07.2026].
- GUS. (2023). Społeczeństwo informacyjne w Polsce w 2023 r. <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2023-roku,1,17.html> [dostęp: 30.07.2026].
- GUS. (2024). Społeczeństwo informacyjne w Polsce w 2024 r. <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2024-roku,2,14.html> [dostęp: 30.07.2026].
- GUS. (2025). Społeczeństwo informacyjne w Polsce w 2025 r. <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2025-r-,2,15.html> [dostęp: 30.07.2026].
- IAB. (2017). Prywatność w sieci 2016/2017. <https://www.iab.org.pl/bez-kategorii/raport-prywatnosc-w-sieci-20162017/> [dostęp: 30.07.2026].
- IAB. (2026). Polacy w social media. https://www.iab.org.pl/wp-content/uploads/2026/01/Raport-Polacy-w-social-mediach_IAB_Polska_2026.pdf [dostęp: 30.07.2026].
- KPMG. (2023). Responsible Data Use at a Crossroads: European Citizen's Perspective on Privacy. <https://assets.kpmg.com/content/dam/kpmgsites/es/pdf/2024/01/european-privacy-market-research-2024.pdf.coredownload.inline.pdf> [dostęp: 30.07.2026].
- Lange, R., Wrońska, A., Ładna, A., Kamiński, K., Błazej, M., Jankiewicz, A., Roslaniec K. (2023). Nastolatki 3.0 Raport z ogólnopolskiego badania uczniów i rodziców. NASK – Państwowy Instytut Badawczy. <https://www.nask.pl/magazyn/nastolatki-3-0-raport-z-ogolnopolskiego-badania-uczniow-i-rodzicow> [dostęp: 30.07.2026].
- PDPC. (1948). Powszechna Deklaracja Praw Człowieka. <https://libr.sejm.gov.pl/tek01/txt/onz/1948.html> [dostęp: 30.07.2026].
- Special Eurobarometr. (2021). Digital Rights and Principles 518. https://data.europa.eu/data/datasets/s2270_96_1_518_eng?locale=en [dostęp: 30.07.2026].
- Wirtualne Media. (2022) Czołowe Komunikatory w styczniu 2022 r. <https://www.wirtualnemedial.pl/te-dwa-komunikatory-dominuja-w-polskim-internecie-discord-przed-telegramem-i-zoomem,7215117734345376a> [dostęp: 30.07.2026].